HYPER-V: VIRTUALIZACIÓN en Microsoft Windows Server 2008

NEX IT

SPECIALIST

REVISTA DE NETWORKING Y PROGRAMACIÓN

$10,80 EN TODO EL PAIS

#45

WiMAX
La solución inalámbrica

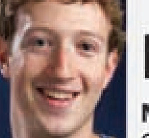
OPEN HARDWARE
Un nuevo movimiento

TECNOLOGÍA xDSL
Su evolución

analizamos las mejores

SUITES DE SEGURIDAD

INNOVADORES ICT



CONOZCA A LOS MEJORES

Mark Zuckerberg
Creador de Facebook

WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00045
Correo Argentino FRANQUEO A PAGAR Cta. 16185
Foto: (c) istockphoto.com/Emrah Turudu

El futuro del DATACENTER

NEX IT SPECIALIST - STAFF

DIRECTOR
- Dr. Carlos Osvaldo Rodríguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

COORDINACIÓN EDITORIAL
- María Delia Cardenal
- Carlos Rodríguez

SENIOR SECURITY EDITOR
- Carlos Vaughn O'Connor

DEPARTAMENTO COMERCIAL
- Ignacio Tellería
itelleria@nexweb.com.ar

EDITORES TÉCNICOS
- Thomas Hughes
- Ariel Cortéz
redaccion@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- Florencia Mangiantini
- Carlos Rodríguez Bontempi

ATENCIÓN AL CLIENTE
- Samanta Casado Arroyo

DISTRIBUCIÓN
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Ernesto Quirino
- Pablo Rivas
suscripciones@nexweb.com.ar

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Huesca Distribuidora de Publicaciones S.A. Aristóbulo del Valle 1556/58. C1295ADH - Capital Federal Argentina. (www.distribuidorahuesca.com.ar)
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1 C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Singularity OS

#45

En sus últimos blogs (www.zdnet.com) Mary JO Foley nos introduce en el sistema operativo Singularity OS, mientras que Christopher Dawson nos cuenta sobre las expectativas que el mismo crea en el ámbito educacional.

Basándome en la información de esos artículos les cuento de qué se trata:

Microsoft ha liberado código como prueba de concepto de un nuevo sistema operativo: Singularity OS. Éste fue construido desde cero y es un desarrollo completamente ajeno a Windows. M. J. Foley comenta que las versiones próximas de Singularity serán diseñadas para testear tecnologías alrededor de procesadores multicore, pero pareciese que también podría ser muy interesante para su uso en las UMPCs (Ultra-Mobile PCs) con procesadores single-core.

Singularity podría ser una alternativa para productos como la Classmate PC de Intel, Eee de Asus o XO PC del proyecto OLPC, en lugar de utilizar un XP degradado como se hace en la actualidad.

Singularity no sacará a Linux del mercado, es solo una prueba de concepto y Linux es un excelente SO aún con mucha vigencia. Pero la idea de tener un sistema operativo Microsoft creado de cero, con un kernel flexible y customizable que pudiese por ejemplo ser adaptado a proyectos que necesitan poco consumo y que fácilmente se pueda escalar a aplicaciones que usen procesadores multicore, es para tener en cuenta.

Singularity es también un vehículo para los procesos llamados SIPs (Softwares Isoltated Processes) que resultan en overheads de performance mucho más pequeños que los actuales "harware-protection schemes" utilizados por los SO de los últimos 40 años. Se estima que podrían obtenerse reducciones del 30 por ciento.

Además ofrece interesantes mejoras en:

- **Seguridad:** sin la necesidad de overheads de software anti-malware (como puede obtenerse usando sistemas Unix) darían mejoras necesarias para, por ejemplo, computadoras del tipo XO.

- **Transparencia de código:** que permitiese customizaciones regionales y poder portarlo a una variedad de hardwares, lo que le permitiría a grupos locales de alrededor del mundo obtener lo que desean del SO y construir aplicaciones customizadas, por ejemplo para el ámbito educativo.

Los dejo entonces con la novedad para que sigan a partir de aquí la evolución de Singularity. Es claro que Microsoft se modificará (ya lo está haciendo) y mutará su estrategia como big player en las TICs (SaaS, datacenters propios, publicidad online, entre otros cambios). Será interesante ver qué rol jugará Singularity en este nuevo escenario. ●

Dr. C. Osvaldo Rodriguez

LOS H

La confiabilidad que necesita

EDICIÓN ESPECIAL



Fundación Favaloro: de Linux a la confiabilidad de Windows Server

Con la plataforma integrada Microsoft, agilizó la carga de información, consolidó el monitoreo de las aplicaciones y ganó en seguridad y confiabilidad.

Después de migrar sus estaciones de trabajo y servidores que corrían sobre Linux a la nueva generación de Windows Server System, Windows XP y Office 2003, Fundación y Universidad Favaloro incrementaron su capacidad de transacciones y los niveles de confiabilidad de la plataforma informática. A su vez, redujeron significativamente los costos de administración de sistemas.

En 2005 las dos organizaciones dedicadas a la atención e investigación en cardiología, experimentaron un fuerte crecimiento tanto en cantidad de servicios médicos y pacientes como en volumen de facturación, lo que hizo colapsar su operatividad. La plataforma informática había llegado al límite de su capacidad de procesamiento de transacciones reduciendo así su posibilidad de interoperar con otros sistemas. Mientras la Fundación se manejaba con productos Microsoft, la Universidad tenía servicios basados en Linux. La decisión entonces fue implementar Windows Server System para contar con una plataforma integrada que incrementara la interoperabilidad y soportara aplicaciones críticas.

El Gerente de Sistemas de la Fundación, Sergio Navarro, señaló al respecto que la plataforma tecnológica resultó segura y confiable debido a que se lograron optimizar las funciones del sistema y del correo electrónico. "Además —agregó— nos permite usar nuestro sistema de gestión hospitalaria al máximo, con todas las prestaciones y funcionalidades de las últimas versiones, incluyendo soluciones antispam y antivirus."

Continúa en Pág. 3.

Las razones de la elección

"Para la institución fue muy importante elegir un socio tecnológico como Microsoft porque le permitió alcanzar una mayor disponibilidad de la plataforma, sin aumentar los costos de operación, ni los profesionales dedicados en el área de sistemas", comenta Gustavo Marota de TPS, Socio de Negocios certificado Microsoft que ayuda a la Fundación a afrontar sus desafíos tecnológicos.

ECHOS

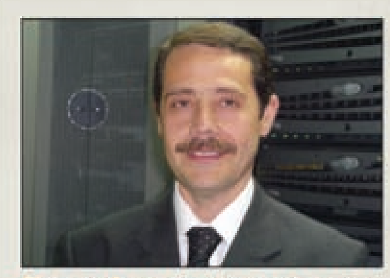
para tomar sus decisiones

Para conocer más sobre este y otros casos visite http://www.microsoft.com/argentina/hechos
o llame al 0800-999-4617





FOTO: P. GONZALEZ



En primera persona

"Ahora tenemos una infraestructura informática mucho más confiable y segura para soportar nuestras aplicaciones críticas. Después de migrar el último servidor Linux a Exchange, no tendremos más servidores Linux en la institución."

Sergio Navarro, *Gerente de Sistemas de Fundación Favaloro*

Excelencia en salud

La Fundación Favaloro es una entidad sin fines de lucro dedicada a la docencia, investigación y asistencia en el terreno de la salud, especialmente en cardiología y otras prestaciones de alta complejidad. Creada en 1975 por el Dr. René G. Favaloro, brinda soporte también a la Universidad. **Pág. 7**

Resultados tangibles

La solución consistió en migrar a Windows Server System (con Microsoft SQL Server 2000, Exchange Server 2003 e ISA Server 2004), Windows XP y Office 2003. Navarro señala que la organización logró aumentar la capacidad transaccional del correo en más de un 67%, y la base de datos en más de un 50%. **Pág. 15**

NOTA DE TAPA



Con millones de virus, malware, programas espías y spam, entre otras muchas amenazas, dando vueltas por la Web, protegerse, prevenirse y armarse para defender nuestra información resulta una tarea vital. Si bien antes era suficiente utilizar un simple antivirus, la veloz evolución y proliferación de nuevas amenazas hicieron que fuera necesario instalar otros softwares de protección en las computadoras.

IT

NOTAS DESTACADAS

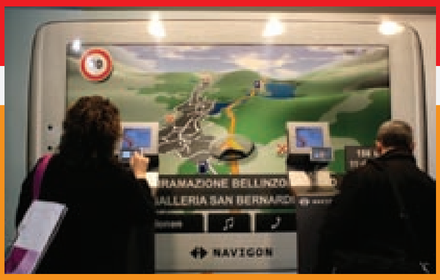


SUMARIO - EDICIÓN #45

EVENTOS

Finalizó CeBIT 2008





La tradicional feria tecnológica de la ciudad de Hannover mostró como puntos más destacados la preocupación por la tecnología verde y las apuestas de los grandes de la industria por los pequeños dispositivos móviles. Con un total de 495 mil visitantes, mucho más de lo que se esperaba en un principio, finalizó en Alemania la más importante y tradicional feria tecnológica de Europa, la CeBIT de Hannover. En está edición hubo un par de temas que se robaron la muestra. El Green IT sin dudas fue uno de ellos, tal cual había ocurrido en enero en la CES de Las Vegas. Es que el tema de la energía y tecnología verde es uno de los temas más en boga en la industria y todos los grandes jugadores vienen apostando por esta tendencia que no solo implica comenzar a preocuparse por el medio ambiente sino también significa importantes ahorros monetarios para aquellas compañías que deciden jugarse por el verde. Así por ejemplo, Intel presentó procesadores que reducen el consumo energético al mínimo y Fujitsu-Siemens monitores TFT que en modo stand by no generan consumo. Kyocera por su parte mostró la impresora C5015N que utiliza un sistema de carga positiva de los tambores, lo que contribuye a frenar la emisión de ozono. Los componentes que usa son de larga duración por lo que no es necesario cambiar el tambor de impresión hasta pasado un ciclo de cientos de miles de páginas. El CEO de Microsoft y una de las presencias estelares de la feria, Steve Ballmer afirmó que las TICs es uno de los sectores que más energía consume, por lo que aseguró que su compañía esta realizando importantes esfuerzos para colaborar en el ahorro de energía y en el cuidado del planeta. En este contexto, la organización Greenpeace tuvo un destacado papel y presencia, otorgando premios para aquellos productos que más se acercaron al ideal del Green IT, materiales renovables y mínimo consumo de energía. Fueron premiados celulares y laptop de Sony, Sony Ericcson, Nokia y Apple. Yannick Vicaire, de Greenpeace, afirmó: "Las manufactureras tienen un largo camino por recorrer, pero poco a poco van tomando conciencia del impacto ambiental de sus productos". La organización del evento se esmeró especialmente para darle color verde a la feria, de manera que un gigantesco sector de la misma llevó por nombre Green IT Village. El otro tema que los organizadores pusieron como base para este año fue el de la necesidad de una integración tecnológica europea en especial entre Alemania y Francia. De hecho el país galo fue el invitado especial este año y su bandera flameó en lo más alto junto a la de los anfitriones. La Canciller alemana Angela Merkel y el presidente francés Nicolás Sarkozy, destacaron en sus discursos que Europa debe unirse inmediatamente para poder afrontar el gran avance de los productos asiáticos en el continente. Paradójicamente, si hubo una compañía que se destacó del resto en esta edición esa fue la taiwanesa Asus. Los creadores de la Eee PC, no solo se destacaron por la renovación de su portátil de bajo costo sino porque llevaron hasta Alemania una gran cantidad y variedad de productos, en especial pequeños móviles. La nueva versión del Eee PC, uno de los productos más vendidos de los últimos tiempos, viene con mejoras en cuanto al tamaño de la pantalla, de 7 a 8,9 pulgadas, al tamaño de la memoria y a la capacidad del disco duro. Además ofrecen la opción de comprarla con XP preinstalado. Las 350 mil unidades vendidas desde su lanzamiento y la tendencia de otras grandes firmas de apostar por portátiles cada vez más livianas y pequeñas, parecen haber convencido a Asus de seguir apostando fuerte por su producto estrella. Y para mostrar que no solo de los productos de bajo costo vive la compañía, en Hannover se presentaron además dos impresionantes dispositivos de lujo, fruto de su acuerdo con Lamborghini, el legendario fabricante de autos italiano. El Smartphone ZX1, basado en Windows Mobile 6, y el portátil ultraligero VX3, cuya carcasa esta fabricada en fibra de carbono. Otros taiwaneses que se destacaron fueron los de Giga vité que presentaron computadoras ultraportatiles, que no obstante ofrecen gran cantidad de prestaciones. Los chinos de Meizu por su parte, también tuvieron protagonismo ya que presentaron el M8, una especie de clon del iPhone pero de bajo costo. Otra de las vedettes de la feria fue la tecnología de navegación GPS. ●



Abril		
2	**Conferencia Latinoamericana CTIA Wireless 2008**	www.ahciet.net
8	**Jornada Trabajo Ingeniería** - *A confirmar*	www.worktec.com.ar
10	**4to Seminario de Segu-Info** *UTN - Facultad Regional Santa Fe*	www.segu-info.com.ar
22	**IDC Argentina SOA & Business Integration Conference**	www.idclatin.com/argentina
16	**Snoop Update 2008** / *A confirmar*	www.worktec.com.ar www.update08.org
27 al 30	**WinConnection**	www.worktec.com.ar www.update08.org
Mayo		
2 y 3	**Centro Libre - Jornadas del Software Libre**	www.centrolibre.org
8 y 9	**Green IT**	www.greenituk.com
8	**Jornada Trabajo IT**	www.worktec.com.ar
20	**IDC Argentina Innovative ERP for the Mid-sized Business Seminar**	www.idclatin.com/argentina

EMPRESA EFICIENTE GARANTIZADA

CONSERVACIÓN DE LA ENERGÍA
Aproveche los beneficios de un sistema de energía eficiente dimensionando adecuadamente su infraestructura, y pagará sólo lo que necesite.

ENFRIAMIENTO ESTRECHAMENTE ACOPLADO
Logre mayor eficiencia térmica con la arquitectura de refrigeración InRow™. Reduciendo la distancia a recorrer por el aire frío (de 15 m a 1,5 m), se elimina la mezcla del aire extraído caliente con el aire frío de la sala, y se vuelve viable un sistema de enfriamiento de precisión más dirigido.

ADMINISTRACIÓN DE LA CAPACIDAD
Administre sus sistemas con máxima eficiencia mediante el software inteligente e integrado para administración de la capacidad, con datos exactos y en tiempo real sobre dónde refrigerar y a qué suministrar energía.

Presentamos Efficient Enterprise™: más energía, más control, más ganancias.

¿Acaso su sistema actual puede ofrecerle lo mismo?

Los potentes sistemas legados funcionan bien cuando se trata de enfriar salas completas, pero los altísimos costos de la energía hacen que elegirlos resulte irresponsable desde el punto de vista físico, y el sobredimensionamiento inherente a su diseño los vuelve inadecuados para enfrentar los desafíos actuales en materia de alta densidad. Para un problema simple, una solución simple. Reduzca sus costos de energía y refrigeración, y utilice los ahorros para comprar los equipos informáticos que necesita. Según la firma Gartner Research, el 50% de los centros de datos construidos antes de 2002 serán obsoletos para 2008 debido a su deficiente capacidad para suministrar energía y refrigeración. El problema más importante que enfrentan los gerentes de data centers actualmente se relaciona con la energía y refrigeración.

Efficient Enterprise™ de APC-MGE.
Esta solución de APC-MGE. para empresas eficientes le permite aprovechar sus recursos al máximo. Escalabilidad modular, para que sólo pague por lo que use, administración de la capacidad que le permite saber dónde ubicar él próximo servidor, y sistemas por hilera y de contención de calor dedicados que aumentan la predecibilidad de los niveles térmicos y de refrigeración. La arquitectura Efficient Enterprise le hace ganar dinero ayudándolo a eliminar los gastos excesivos. Por ejemplo, con sólo pasar de un esquema de refrigeración para toda la sala a uno por hilera, ahorrará en promedio 35% en costos de electricidad.

Nuestro sistema le devuelve su dinero
Ya sea que construya un centro de datos nuevo o analice la eficiencia de sistemas existentes, lo primero que debe saber es dónde está parado. Aproveche el servicio online de Auditoría de Efficient Enterprise™ para saber cómo obtener beneficios con un sistema inteligente, integrado y eficiente: más energía, más control, más ganancias.

CONTENCIÓN DEL CALOR
Eleve sus niveles de eficiencia con el esquema de refrigeración conteniendo el calor y eliminando la costosa contaminación cruzada de temperaturas. Nuestro sistema de contención de pasillo caliente reduce los costos operativos hasta un 50% respecto de los enfoques basados en sistemas legados.







¿Qué grado de eficiencia tiene su sistema corporativo?

Sepa exactamente dónde está parado: aproveche el servicio de Auditoría de la eficiencia de la empresa hoy mismo.

Visite www.apc.com/promo Código 63488d • Llame al 0-800-222-3232

nexmedia.com.ar

NOTICIAS

Intel presenta Atom, su procesador de bajo consumo

En el que fue definido por la misma compañía como el lanzamiento más importante desde el procesador Pentium, Intel presentó Atom un procesador enfocado hacia los dispositivos móviles.

TIPS

Cómo elegir la Laptop adecuada

Seis claves que nos ayudaran a elegir la laptop ideal para nuestras necesidades, en medio de la gran cantidad de ofertas y variedad de productos que nos ofrece el mercado.

Cómo mejorar una conexión wireless

Lo primero y principal es encontrar una buena antena para el router; esto incrementará el poder de la señal en un 15 ó 20 por ciento como mínimo…

BUSINESS IT

Microsoft y Google ahora se disputan el mercado de la información médica

Ambas compañía han comenzado a ofrecer servicios para que los usuarios almacenen y gestionen sus datos médicos a través de Internet.



EDUCACION

Primer Posgrado de Calidad en Software

La carrera creada por el INTI, tiene una duración de dos años, apunta a paliar la falta de recursos humanos especializados en IT, se dictará en la Universidad Nacional de San Martín.



GADGETS

Nokia Morph

Descubrí a través de fotos, video y nota el impresionante Nokia Morph, un nuevo dispositivo desarrollado por Nokia y la Universidad de Cambridge que utiliza las ventajas de la nanotecnología y que muestra que en un futuro cercano los móviles serán fabricados con materiales tan flexibles que se podrán modificar de tamaño y forma a nuestro antojo.



El futuro del DataCenter

¿Dónde está el DataCenter en la actualidad? ¿Cuál será su papel en los próximos años? ¿Cómo evolucionará? ¿Cómo influirá la virtualización en la forma de almacenar nuestra información? ¿Cómo mejorar y optimizar nuestro centro de datos? Estas son algunas de las preguntas que Cisco le realizó a Zeus Kerravala, Vicepresidente Senior de Investigación Corporativa en Yankee Group. Conozca qué piensa.

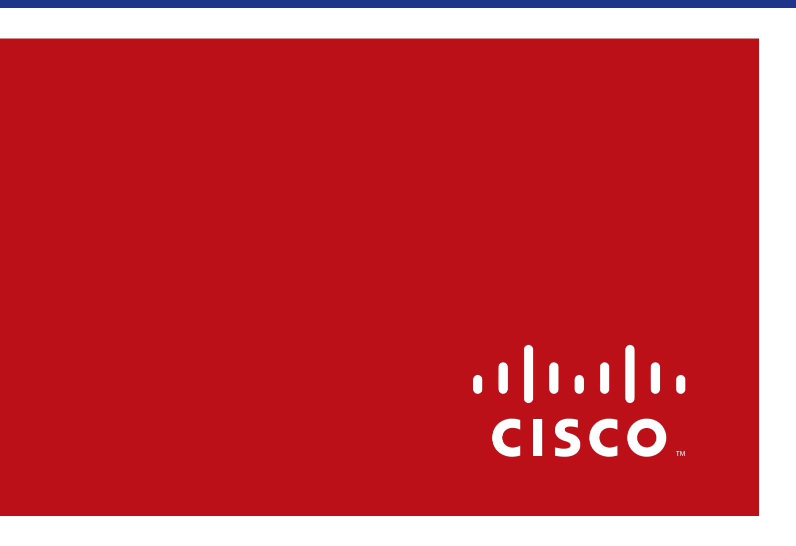
¿CUÁLES SON LAS PRINCIPALES QUEJAS DE LOS CENTROS DE DATOS, SEGÚN LOS ADMINISTRADORES Y EJECUTIVOS IT?

Zeus Kerravala: Hay varios puntos que afectan a los administradores de los centros de datos de hoy. En primer lugar, la actual utilización de los recursos de los data center es muy bajo: una investigación de Yankee Group muestra que la utilización del almacenamiento es sólo del 25 por ciento, el empleo del servidor un 30 por ciento y el uso de la red también, apenas de un 30 por ciento. Dado que las aplicaciones tienden a estar instaladas en silos, cuando un recurso específico está al 100 por ciento de su capacidad, la empresa debe comprar más para una aplicación particular, en lugar de poder emplear el recurso que está siendo subutilizado.

Otro gran desafío es lograr una mejor manipulación de la energía y del enfriamiento. En el año 2000, el número promedio de KW por rack era de 2,5; en 2006 se había incrementado a alrededor de 10 KW por rack y, a la actual tasa de crecimiento, calculamos que en el año 2010 la misma será de más de 30 KW por rack. Esto ha creado un aumento en la cantidad de fondos asignados a la energía y enfriamiento. En 2000, las áreas de energía y enfriamiento se quedaban con aproximadamente el 20 por ciento de los gastos de un nuevo servidor; actualmente esa tasa es de algo más del 50 por ciento y, si nada cambia será de más del 80 en el año 2010. Es evidente que el statu quo no es suficiente y que es necesario cambiar las cosas para afrontar los retos del futuro.



Zeus Kerravala es el Vicepresidente Senior de Investigación Corporativa en Yankee Group. Su expertise incluye el trabajo con clientes para la resolución de problemas corporativos a través del desarrollo de soluciones de infraestructura tecnológica, incluyendo switching, routing, administración de redes, soluciones de voz y VPNs. Antes de unirse a Yankee Group, Kerravala fue senior engineer y technical project manager en Greenwich Technology Partners, empresa de consultoría e infraestructura de redes. Anteriormente fue vicepresidente de IT en Ferris, Baker Watts en donde estuvo a cargo del desarrollo de las soluciones técnicas para las diferentes unidades de la empresa. Kerravala es Licenciado en Física y matemáticas de la University of Victoria (Canadá) y cuenta con certificaicones de Citrix y NetScout.



¿Qué tipo de innovaciones creen ustedes que habrá a futuro para ayudar a los administradores de centros de datos a abordar sus cuestiones más urgentes?

Zeus Kerravala: Habrá innovaciones en muchas áreas. Ya hemos visto el impacto que la virtualización puede tener sobre la eficiencia del servidor. En un entorno bien administrado, la utilización de un servidor virtual ha aumentado de un 30 por ciento a más del 90. La virtualización es una tendencia que está empezando a tener efectos sobre el almacenamiento y que en breve también influirá sobre la red. Hasta ahora ha sido usada principalmente para hacer que un servidor parezca muchos servidores. Eventualmente, la virtualización desempeñará un papel diferente y desglosará completamente al servidor. En lugar de tener una caja física con almacenamiento, CPU, memoria, etc., incorporados en ella, la virtualización le permitirá al servidor estar formado por componentes virtuales. También esperamos ver mejoras en la eficiencia energética, de manera tal que los servicios de centro de datos sean servicios virtuales que se sirven fuera de la red. Así, en lugar de instalar una nueva pieza de hardware cada vez que un nuevo recurso es necesario, el administrador del centro de datos será capaz de poner a funcionar el servicio. Con respecto a la refrigeración, esperamos ver nuevos métodos de refrigeración para el equipamiento del centro de datos, incluidos los servidores refrigerados de líquidos para enfriar cosas como racks de servidores blade.

¿Cuáles son algunas de las áreas clave en las que la red puede agregar valor a los centros de datos de próxima generación?

Zeus Kerravala: La red desempeña un papel muy importante en el data center virtualizado. En primer lugar, es pervasiva y afecta a todos los diferentes recursos de un centro de datos. Es el recurso que permite a las aplicaciones conectarse a los diversos grupos de recursos informáticos. Debido a esto es que se espera más y más de la red. El mantenimiento de las ventanas se reducirá o se transformará en inexistente, por lo que la red necesita estar continuamente a su disposición y ser capaz de proveer recursos de manera dinámica cuando y donde sean necesarios. El paso hacia una arquitectura orientada a servicios (SOA) quedará habilitado por la red, en la medida en que ella es el lugar óptimo a partir de la cual se distribuyen los recursos SOA. Por último, la red va a ser el motor de la aplicación de políticas que aseguren que los recursos de los centros de datos estén siendo utilizados de la manera más eficiente posible.

El aumento masivo de datos y la proliferación de las aplicaciones y tecnologías Web 2.0 han tenido un gran impacto en cómo las empresas gestionan sus datos y sus data centers. ¿Podría mencionar algunas de las estrategias que están brindando mayor éxito?

Zeus Kerravala: La proliferación masiva de datos ha hecho que las empresas examinen seriamente la forma en que se gestionan los data centers. Como se dijo anteriormente, la utilización de los recursos del centro de datos es muy pobre y sus administradores simplemente no pueden continuar agregando elementos y haciendo caso omiso de los recursos que están subutilizando. Esto ha originado un aumento en el uso de tecnologías de virtualización, sistemas de almacenamiento y servidores blade. Por supuesto, estas tecnologías son sólo tan buena como los instrumentos de gestión que permiten a los administradores de data centers administrar estos recursos con la mayor eficacia posible. Esperamos ver más innovación en las herramientas de gestión, a medida que las tecnologías de los centros de datos continúen evolucionando.

¿Qué rol cree usted que jugará la red, a medida que los data centers vayan evolucionando?

Zeus Kerravala: Así como el centro de datos evoluciona, también lo hará la red. El data center virtualizado del futuro se basará en grupos de recursos que estarán interconectados por la red. En esencia, la red se convertirá en el backplane o placa madre del centro de datos virtual, y jugará muchos papeles. La red será la aplicación fluente y el motor de orquestación de servicios que regirán qué recursos irán a qué aplicaciones. La red será el espacio donde residirán muchos servicios SOA, y la red automáticamente brindará los recursos cuando y donde sean necesarios.

¿Cómo cree usted que se verá un data center dentro de 5, 10 años?

Zeus Kerravala: De aquí a 5, 10 años los centros de datos se verán drásticamente diferentes. Hoy cada uno está altamente individualizado, y posee recursos informáticos que se dedican a aplicaciones específicas. En el centro de datos del futuro, todos los recursos se habrán transformado, yendo desde una infraestructura física hacia una infraestructura virtual. Memoria, almacenamiento, procesador, base de datos (entre otros recursos informáticos) serán recursos virtuales que podrían denominarse "a la carta" (on demand) por cualquier aplicación, cuando así lo requiera. Estos recursos virtuales estarán compuestos por un conjunto de los recursos físicos que pueden atravesar al data center, a través de la ciudad o a través de todo el mundo, pero que se verá como un único recurso para todas las aplicaciones. Esto impulsará la utilización de los recursos del centro de datos desde cerca de un 20 por ciento (donde se ubica hoy) hasta más del 90 por ciento. En 5, 10 años los data center también serán aprovechados al máximo por el poder y la eficiencia de enfriamiento, en la medida en que Green IT se vaya convirtiendo en un mandato corporativo para todas las organizaciones. ●

NOTA #2

TECNOLOGIAS xDSL

Las tecnologías de la familia xDSL han evolucionado de forma tal que han posibilitado un desarrollo sostenido en el acceso a Internet en los últimos años. En gran medida esto se debe a la versatilidad que provee esta tecnología para brindar altas velocidades de transmisión de datos a costos accesibles.

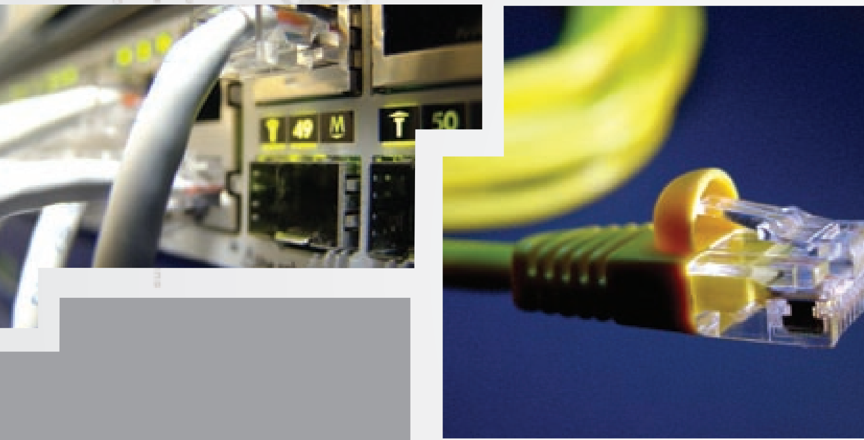


FOTO: http://www.sxc.hu/ Darren Hester / Andrew Brigmond

Autor:
Miguel F. Lattanzi
Ing. en Telecomunicaciones (IUPFA)

La tecnología DSL (Digital Subscriber Line) provee a los usuarios de un acceso de datos multimedia a alta velocidad, sacando ventaja del uso del par de cobre existente, permitiendo reutilizar el cableado telefónico ya instalado.

Existen varios tipos de tecnologías DSL, las cuales fueron desarrolladas a lo largo del tiempo para adaptarse y cumplir con los requerimientos de los clientes.

En su conjunto forman lo que se conoce como la familia de tecnologías xDSL, donde la "x" es reemplazada por la primera letra de la tecnología en cuestión.

Fundamentos de DSL

Las tecnologías de acceso analógico sobre par de cobre están limitadas por el rango de frecuencias que pueden utilizar, lo cual se traduce a un ancho de banda efectivo muy restringido. Con un ancho de banda acotado, se obtienen bajas velocidades de transmisión de datos, lo cual finalmente se traduce a que los usuarios finales tendrán un servicio "lento", técnicamente hablando, con poca capacidad de transmisión de información. Las tecnologías DSL –digitales como su sigla lo expresa– utilizan un rango de frecuencias mayor que el utilizado por la tecnología analógica dial-up (acceso telefónico por MODEM); lo que permite establecer un canal de comunicación con mayor capacidad. Al tener un canal de gran capacidad, se obtienen altas velocidades de transmisión de datos. Cabe mencionar que estas tecnologías utilizan las técnicas de modulación como base para alcanzar dichas velocidades.

Ancho de Banda vs. Velocidad

Ancho de banda se refiere al rango de frecuencias utilizado, magnitud que se mide en Hertz [Hz]. Por otro lado, la velocidad de transmisión de un canal de comunicaciones es la tasa de bits que pueden ser transmitidos por unidad de tiempo se la mide en bits por segundo [bps]. Es importante diferenciar ambos conceptos dado que a menudo se confunden o se los denomina de forma errónea.

Debido a que DSL utiliza un ancho de banda mayor que dial-up, se le da el nombre popular de "banda ancha", lo cual técnicamente no es incorrecto.

En la figura 1 se puede apreciar el espectro utilizado por una señal de ADSL (Asymmetric Digital Subscriber Line). Se puede observar una componente de frecuencia que abarca de 0Hz a 4KHz, dicho rango de frecuencia se utiliza para la transmisión de las señales telefónicas para el transporte de la voz.

A continuación existe un rango de frecuencia de alrededor de 20KHz, comprendido entre los 4KHz y 25KHz que se denomina "banda de seguridad" o de protección. Es una división

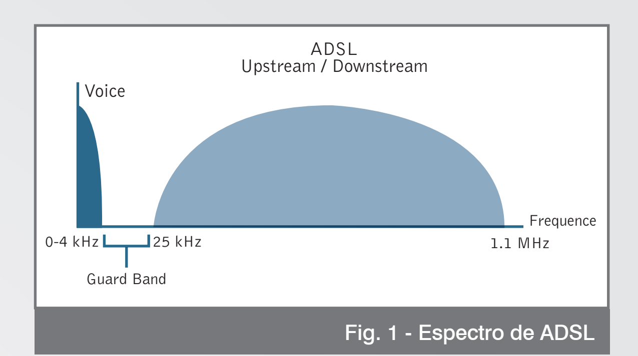


Fig. 1 - Espectro de ADSL

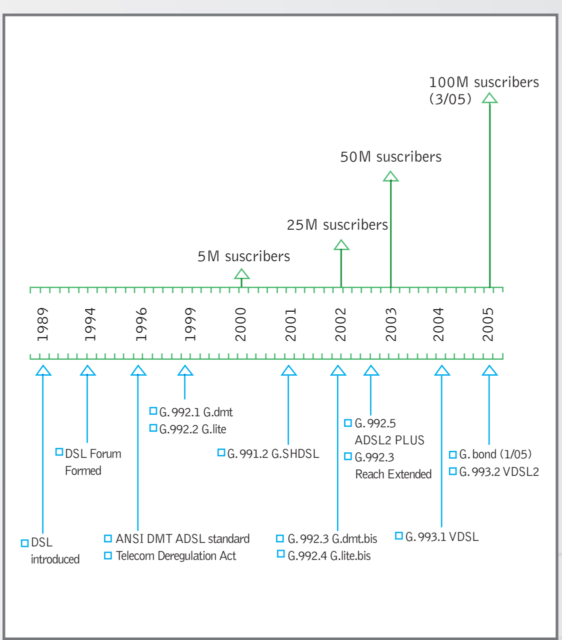


Fig. 2 - Evolución de los estándares xDSL y el crecimiento del mercado

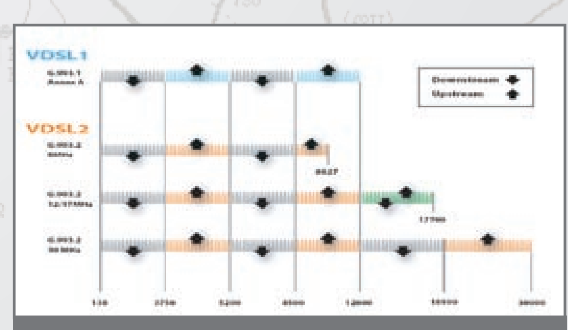


Figura 3 - Espectro VDSL y VDSL2

FOTO: http://www.sxc.hu/ Marco Soscia

en el dominio de la frecuencia que se utiliza para evitar que las frecuencias más bajas de la señal de ADSL interfieran con las frecuencias utilizadas por la señal de voz.
Por último se tiene el rango utilizado por la señal ADSL, comprendido entre los 25KHz y los 1.104KHz (o 1,104MHz).
Este rango de 1,079MHz contiene tanto las frecuencias que se utilizan para enviar información en sentido Upstream (desde el abonado hacia el lado central), como en sentido Downstream (desde la red del proveedor hacia el abonado).
El mismo está dividido de la siguiente manera: de los 25KHz a los 138KHz se concentran las frecuencias utilizadas para la transmisión de datos en sentido Upstream; y de los 140KHz a los 1,104MHz se encuentran las frecuencias utilizadas para la transmisión de datos en sentido Downstream.

Veamos a continuación los distintos tipos de tecnologías xDSL.

Tecnologías xDSL

Como los fundamentos de DSL han sido explicados sobre una señal ADSL, dejaremos un poco de lado los detalles de la señal para ver las principales características del servicio.

ADSL

Es una tecnología de acceso asimétrica, dado que ofrece mayor velocidad de transferencia de datos en sentido Downstream que en sentido Upstream.
En este último se pueden alcanzar velocidades de hasta 1Mbps, mientras que en sentido Downstream de hasta 8Mbps.
Las máximas velocidades de transmisión de datos en ambos sentidos dependen directamente de la distancia del medio físico –recordemos que se utiliza par de cobre–. En la práctica las velocidades mencionadas se pueden alcanzar hasta unos 2,5Km de la central, con una planta externa en muy buenas condiciones.
Como es sabido, todas las señales de telecomunicaciones se degradan conforme viajan por el medio físico que sirve como transporte, lo cual se debe al fenómeno de atenuación, que es la perdida de potencia –o amplitud– de una señal a medida que ésta se aleja de la fuente que la generó.
La atenuación afecta a las tecnologías xDSL de forma no lineal, a medida que la distancia aumenta al doble (se duplica) las tasas de transmisión de datos de Upstream y Downstream se reducen en un factor de cuatro. Entonces, por ejemplo, a 5Km de la central se podrán alcanzar como máximo velocidades del orden de un cuarto (1/4) de las que se alcanzan a 2,5Km.
ADSL es una tecnología que satisface las necesidades de un servicio con altas velocidades de descarga de datos, como ser, servicio de VoD (Video on Demand), Home Shopping, acceso a Internet por banda ancha y e-learning.

- Estándar ITU-T G.992.1
- Upstream: 1Mbps – Downstream: 8Mbps
- Ancho de Banda: 1,104MHz

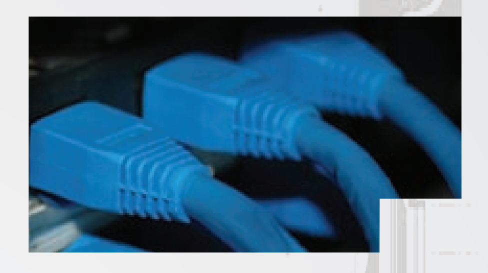
ADSL2

Al igual que ADSL, es también una tecnología asimétrica, que permite aún mayores velocidades de transmisión de datos en sentido Downstream manteniendo la capacidad de transmitir 1Mbps en sentido Upstream.
La máxima velocidad de transmisión que se puede obtener de bajada es de 12Mbps, lo que representa un incremento del 50 por ciento respecto de ADSL.
ADSL2 puede alcanzar dichas velocidades debido a una mejora en los códigos de línea utilizados, lo que permite enviar mayor cantidad de información en el mismo ancho de banda que ADSL (1,1MHz).
A pesar del mejor rendimiento, esta tecnología no fue tan ampliamente implementada como ADSL, como principal motivo se puede destacar que ADSL2+ se lanzó al mercado en un tiempo relativamente corto desde el lanzamiento de ADSL2, con lo cual la tendencia general fue migrar directamente de ADSL a ADSL2+.
Esta tecnología permite brindar los mismos servicios que ADSL, prestando un mejor rendimiento a aplicaciones de video que requieran aun más capacidad de transmisión.

- Estándar ITU-T G.992.3
- Upstream: 1Mbps – Downstream: 12Mbps
- Ancho de Banda: 1,104MHz

ADSL2+

A diferencia de ADSL2, está tecnología soporta mayores velocidades en sentido Downstream por utilizar un ancho de banda mayor en conjunto con mejoras tecnológicas.
Usa un espectro de frecuencias que comprende hasta los 2,2MHz, duplicando de esta manera al utilizado por las tecnologías precedentes.
En sentido Upstream se pueden alcanzar velocidades un poco mayores a 1Mbps, mientras que en sentido Downstream es posible llegar a los 24Mbps.
Las distancias máximas utilizadas para todas



las implementaciones de la familia ADSL rondan entre los 5Km y 5.5Km.
ADSL2+ es la tecnología de acceso xDSL por excelencia para el soporte de servicios Triple-Play, nombre comercial que se estableció para indicar el uso simultáneo de los servicios de acceso a Internet de alta velocidad, video y voz.
Aquí el servicio de video incluye tanto la componente de VoD –a demanda–, como la componente de IPTV (Internet Protocol TV) que sigue el concepto de multidifusión utilizado por la TV tradicional.
El servicio de voz hace referencia a la tecnología VoIP y sus variantes.

- Estándar ITU-T G.992.5
- Upstream: 1Mbps – Downstream: 24Mbps
- Ancho de Banda: 2,208MHz

DSL Forum

Es un consorcio internacional formado por más de 200 empresas del sector de las telecomunicaciones y tecnologías informáticas. Fue fundado en 1994 y hoy en día conforma un ámbito esencial de discusiones tecnológicas para los proveedores de equipos y de servicios en el mercado de las redes de acceso por banda ancha. A pesar de su función principal relacionada con las tecnologías xDSL, desde 2004 se organizaron nuevos grupos de trabajo para otras tecnologías de acceso con diferentes medios de transmisión, como ser la fibra óptica.

SHDSL

Symmetric High-speed Digital Subscriber Line (SHDSL) es una tecnología de acceso simétrica, es decir, que permite brindar la misma velocidad de transmisión de datos en ambos sentidos.
Es un estándar relativamente nuevo, que fue desarrollado originalmente para servir de convergencia a otras tecnologías simétricas como SDSL, HDSL y HDSL-2, soportando todas las funcionalidades relacionadas con dichas tecnologías.
SHDSL brinda dos modos distintos de operación a nivel de acceso físico, puede operar a 2 ó 4 hilos –uno o dos pares de cobre–.
Trabajando en el modo de 2 hilos (2 Wires), puede desarrollar velocidades comprendidas

entre 192Kbps y 2,304Mbps.
Al operar en modo 4 hilos (4 Wires), físicamente se tienen dos pares de cobre, pero a nivel lógico es como tener un vínculo igual al de dos hilos con mayor capacidad de datos, lo que permite alcanzar velocidades de transmisión más elevadas.
Dichas velocidades se encuentran comprendidas entre 384Kbps y 4,608Mbps como máximo.
Este tipo de tecnología es muy utilizado para aplicaciones que requieran una alta capacidad de transmisión de datos en sentido Upstream o que por sus características necesiten de un medio que brinde un servicio simétrico. Por lo general SHDSL se implementa en segmentos empresariales.
A diferencia de la familia ADSL, en esta tecnología no se contempla el uso del servicio telefónico tradicional, es decir, no existe la asignación en frecuencia del canal de 4KHz utilizado para el transporte de las señales de voz.
En caso de utilizar SHDSL para brindar acceso telefónico tradicional es preciso optar por alguna variante, como ser el caso de VoIP (Voice over Internet Protocol).
Operando a dos hilos se utiliza a una distancia máxima de 3Km y operando a cuatro hilos se realizan implementaciones que involucren una distancia máxima de hasta 5Km.

- Estándar ITU-T G.991.2
- Upstream/Downstream (2w):
192Kbps – 2,304Mbps
- Upstream/Downstream (4w):
384Kbps – 4,608Mbps

VDSL

Very high-speed Digital Subscriber Line (VDSL) es una tecnología que permite tanto la trasmisión de datos de forma simétrica como asimétrica.
Los trabajos para la estandarización de VDSL comenzaron en 1995, pero varios años después no se habían producido grandes avances, principalmente debido a que no se llegaba a un acuerdo sobre qué tipo de modulación utilizar. Después de varios años de idas y vueltas, a finales del 2003 la ITU (Internacional Telecommunication Union) ratificó el estándar G.993.2, teniendo así un documento unificado con todos los requerimientos necesarios para su implementación práctica.
A diferencia de las tecnologías de la familia ADSL, VDSL/VDSL2 no tienen una única banda de frecuencia para Upstream y una para Downstream, sino que combinan varias de estas de forma intercalada.
VDSL utiliza un especto de frecuencia que abarca hasta los 12MHz. Debido a que las frecuencias más altas son más sensibles a los efectos de los parámetros de línea, como la atenuación, las distancias que se pueden alcanzar con las velocidades máximas son pequeñas en comparación con otras tecnologías de acceso xDSL.
Las implementaciones a velocidades de transmisión máximas, en la práctica, se dan a distancias de alrededor de 400m, y es muy difícil encontrar implementaciones que involucren distancias mayores a 1Km.
Debido a su corto alcance VDSL se utiliza principalmente en escenarios MDU (Multi- Dwelling Unit) o MTU (Multi-Tenant Unit), en los cuales se llega por otro medio –como ser fibra óptica– a un equipo concentrador de acceso que brinde las interfaces necesarias para implementar vínculos VDSL hacia los abonados.

- Estándar ITU-T G.993.1
- Upstream/Downstream: 26Mbps
- Upstream: 12Mbps – Downstream: 52Mbps
- Ancho de Banda: 12MHz

VDSL2

El estándar de VDSL2 se ratificó por medio de la ITU en mayo de 2005, como objetivo principal se buscó generar una tecnología que permitiese incrementar el alcance de servicios con velocidades de transmisión de datos mayores a 25Mbps más allá de 1Km, y que sirviera de soporte para servicios de acceso simétrico a 100Mbps en distancias menores de 350m.
Utiliza un rango de frecuencia mayor al de VDSL, llegando a los 30MHz del espectro de frecuencia.
VDSL2 es el estándar más complicado que haya confeccionado la ITU para redes de acceso xDSL. La especificación es compleja desde el punto de vista tecnológico, por contener muchas variables que se combinan y cambian en sí mismas con otras variables.
En gran parte, el éxito en la estandarización de VDSL2 se debe al avance tecnológico de los últimos años en los servicios de video, en especial HDTV (High Definition TV).
Si se toma como promedio que cada canal de HDTV es codificado en 15Mbps, y planificando una red basada en dos TV por hogar, se tienen 30Mbps sin tener en cuenta el acceso a Internet por banda ancha y el posible servicio de VoIP.
Esto deja bien en claro que los 24Mbps que brinda ADSL2+ no son suficientes, y que los 52Mbps que brinda VDSL parecerían quedar ajustados si se brindan servicios de acceso LAN-to-LAN a 10Mbps, en conjunto con los ya mencionados anteriormente.
Además de ser la mejor tecnología de acceso para los servicios de video, VDSL2 se está implementando como conexión simétrica de alta velocidad, principalmente en el segmento empresarial o SOHO (Small Office/Home Office).

- Estándar ITU-T G.993.2
- Upstream/Downstream: 100Mbps
- Upstream: 45Mbps – Downstream: 85Mbps
- Ancho de Banda: 30MHz

Resumen

De lo expuesto anteriormente, se concluye que hoy en día existen un gran número de tecnologías de acceso xDSL que se amoldan a los diferentes requerimientos por parte de los usuarios, desde el segmento empresarial al segmento hogareño.
Desde el punto de vista de los servicios se puede observar cómo la tecnología necesaria para brindarlos ha avanzado de la mano de estos e inclusive más allá.
Por otro lado muchas aplicaciones on-line, como los sitios de broadcasting de video –de los cuales YouTube es de los más populares– o los servidores de juegos, han surgido aprovechando las altas velocidades de transmisión que llegan a muchos hogares en forma masiva.
Todos los aspectos desarrollados en el presente artículo tienden a clarificar y presentar los tipos más utilizados de tecnologías xDSL en la actualidad, vale aclarar que dichas tecnologías son implementadas por equipos de telecomunicaciones, que en su conjunto forman la red de acceso y permiten brindar todos los servicios mencionados.
En el próximo artículo de la serie “Redes de Acceso” se presentará, desde el punto de vista operativo, como se implementan las tecnologías de la familia ADSL en cuanto a los equipos utilizados, su topología de red y los protocolos que intervienen. ●

Notas de la Serie

#1 Evolución en el Acceso

#2 Tecnologías xDSL

#3 Implementación de ADSL

#4 Fibra Óptica en el Acceso

#5 Tecnologías xPON

Aprendiendo con los expertos:

WINDOWS SERVER

Particiones de Active Directory

Autor:
Lic. Silvana Del Roscio
Analista de Sistemas
MCT / MCSE

¿Dónde se encuentran los archivos del Active Directory? ¿Qué son las particiones?

Al configurar a un servidor como controlador de dominio, uno de los datos solicitados por dcpromo.exe es dónde ubicar a la base de datos y a sus archivos de registro. La ubicación predeterminada es c:\windows\NTDS.
Terminada la "promoción" a controlador de dominio encontraremos allí a los siguientes archivos:

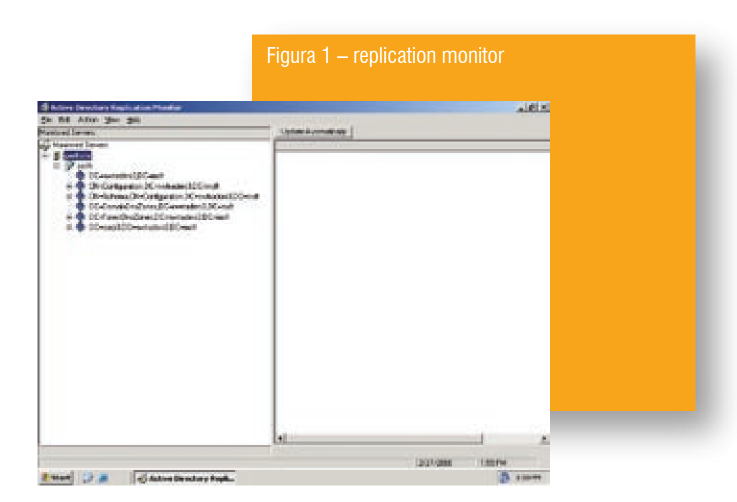
ntds.dit *La base de datos (la extensión DIT se refiere a Directory Information Tree)*
edb.log *Archivo de registro de transacciones*
res.log* *Archivos de reserva para el archivo de registro*
edb.chk *Archivo de comprobación o checkpoint.*

Todos los cambios que hacemos sobre los objetos se graban primero en memoria, luego se registran en el archivo de log y finalmente en el archivo de base de datos. Cuando ya se actualizó la base de datos se actualiza también el archivo de comprobación (para llevar control de qué falta traspasar del archivo de log a la base).

Es fundamental hacer backup de estos archivos!

El backup del Active Directory se hace al hacer un backup de lo que se llama System State Data, que incluye, entre otras cosas, también a la carpeta SYSVOL (que es donde se almacenan las políticas), al registro y a los archivos de inicio.
En la herramienta Backup (Start – Programs – Accesories – System Tools – Backup o directamente, Start – run – ntbackup), hay que elegir Advanced Mode – Backup y System State.
La base de datos de Active Directory está lógicamente "separada" en particiones.
Estas son: la partición del schema, la partición de configuración, la partición del dominio y particiones de aplicación.
Las vemos al usar utilitarios que ayudan a obtener información sobre el estado de la replicación, como por ejemplo Replication Monitor (replmon.exe, que se instala al instalar las herramientas de soporte). Presionando botón derecho sobre Monitored Servers podremos agregar un servidor, y presionando nuevamente botón derecho, esta vez sobre el servidor, tendremos la posibilidad de chequear topología de replicación, estado, averiguar qué servidores son servidores de catálogo global, etc.
También podremos ver referencias a estas particiones en los mensajes de error de replicación que aparecen en los archivos de registro del Event Viewer.

Figura 1 – replication monitor



Entender qué es cada una de ellas, qué información almacenan y el alcance de su replicación podrá ayudar a interpretar mejor un error, como asi también conocer un poco más sobre el servicio de directorios que estamos usando.
La partición del schema, como su nombre lo indica, contiene al "schema", que es el conjunto de definiciones de todos los objetos y atributos que pueden crearse en el directorio. El schema es único para todo el forest (bosque), por eso, esta partición se replica a todos los controladores de dominio del bosque. Para entender mejor qué es el schema, podemos usar la herramienta Active Directory Schema, un complemento de MMC que no está disponible sin antes hacer la registración de una dll. (en la línea de comandos, ejecutar regsvr32 schmmgmt.dll).
Una vez hecha la registración, podremos agregar el complemento (snap

Figura 2 – registración de .dll

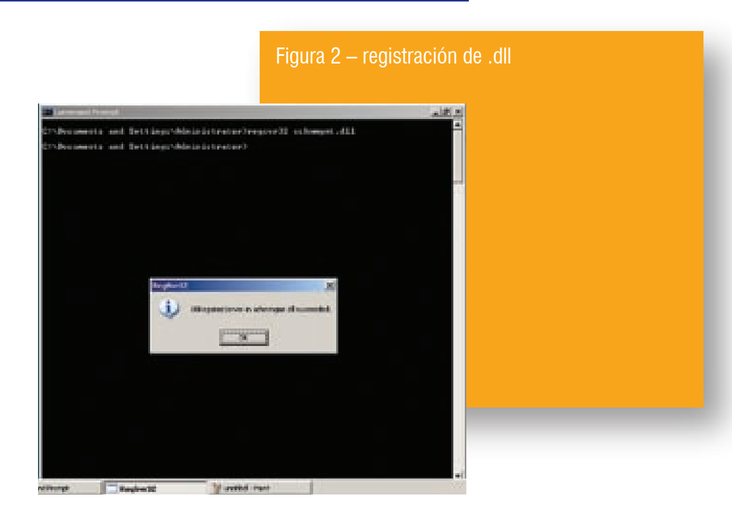
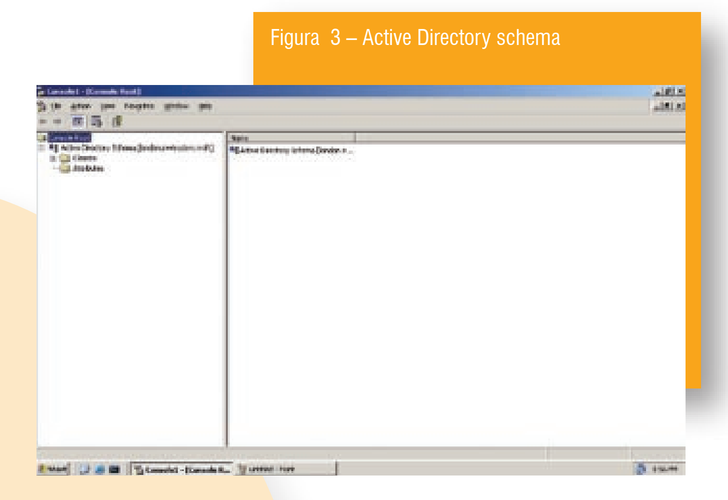


Figura 3 – Active Directory schema



in) en MMC. (Inicio - Ejecutar - mmc - Add/Remove Snap Ins - Add - Active Directory Schema).
Las clases definen qué objetos pueden crearse (usuarios, computadoras, grupos) y los atributos definen las propiedades de esos objetos. Por ejemplo, para un usuario asignamos un "logon name", un "full name", "title", etc.
Siendo el esquema único para todo el bosque, se garantiza que todos los objetos de dicho bosque se crearán respetando las mismas reglas.
La partición de configuración también es única para todo el forest y se replica a todos los controladores de dominio de dicho forest. Contiene información sobre la estructura del Active Directory, incluyendo dominios, sitios y controladores de dominio existentes en el forest. De esta manera, todos los controladores de dominio "conocen" cómo es el árbol y el forest al cual pertenecen como así también la definición de la estructura física definida mediante los sitios.

La partición del dominio contiene información sobre los objetos propios del dominio (usuarios, grupos, computadoras, unidades organizativas,etc). Se replica a todos los controladores de dominio del DOMINIO.
Ejemplo:

dominio padre	**A.com**	**1 Controlador de Dominio (DC1)**
dominio hijo	**B.A.com**	**2 Controladoree de Dominio (DC2, DC3)**

DC1, DC2 y DC3 replican entre sí la partición de Schema y de Configuración. DC2 y DC3 replican entre sí la partición del dominio B.A.com Si DC1 es el servidor de catálogo global, recibirá también una réplica parcial de la partición del dominio B.A.com. Una réplica parcial significa que recibe la lista total de objetos pero con un subconjunto de propiedades (no todas, sino sólo aquellas más utilizadas en las búsquedas).
Anteriormente mencionamos a las particiones de aplicación. Una aplicación que puede almacenar sus datos en Active Directory es DNS. Si el servidor de DNS es controlador de dominio, al crear una zona tenemos la opción de elegir "Store the zone in Active Directory". Si la seleccionamos en la pantalla siguiente se nos pedirá configurar el alcance de la replicación de los datos de la zona que estamos creando.

Las opciones son:

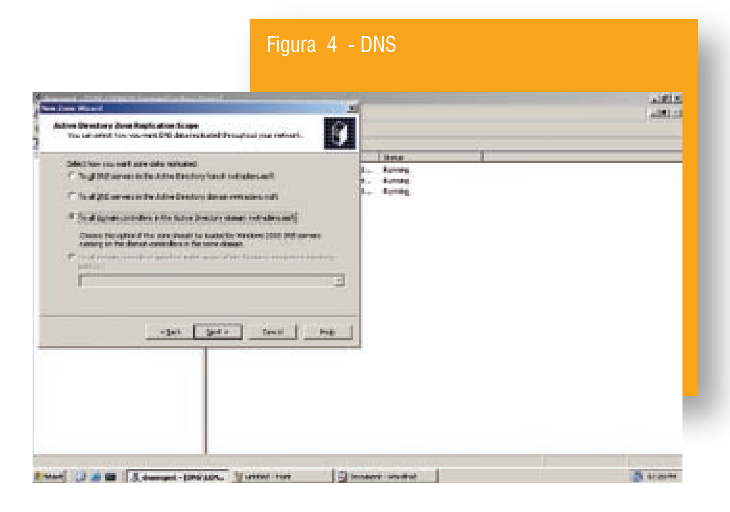
To all DNS Servers in the active directory forest
Los datos de la zona se replicarán a todos los controladores de dominio de todo el forest que además sean servidores de DNS. La partición de aplicación que almacena estos datos se llama ForestDNSZones y es una para todo el forest.

To all DNS servers in the active directory domain
Los datos de la zona se replicarán a todos los controladores de dominio del dominio que además sean servidores de DNS. La partición de aplicación que almacena estos datos se llama DomainDNSZones y es única para cada dominio.

To all domain controllers in the active directory domain
Los datos de la zona se replicarán a todos los controladores de dominio del dominio (sean o no servidores de DNS) como parte de la partición del dominio.

To all domain controllers specified in the scope of the following application directory partition
Esta opción estará deshabilitada si previamente no creamos una partición de aplicación.
Deberíamos crear una partición de aplicación (con el comando dnscmd.exe, por ejemplo) y luego agregar al servidor a la lista de servidores que participan de la replicación de esta partición (también puede hacerse con el comando dnscmd.exe). Esta opción es para controlar aún más el tráfico asociado a la replicación de los datos de DNS. ●

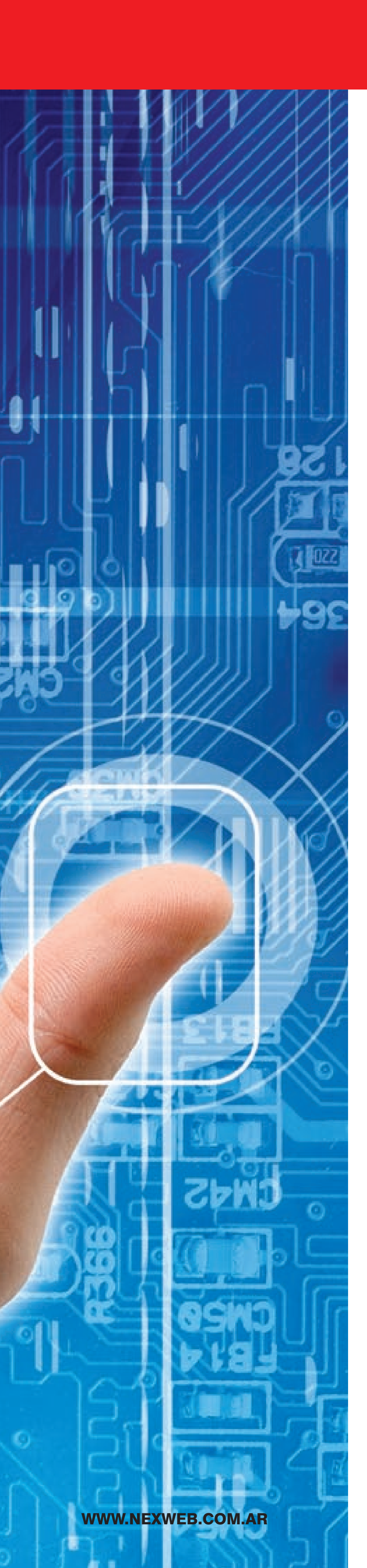
Figura 4 - DNS





SUITES DE SEGURIDAD

Con millones de virus, malware, programas espías y spam, entre otras muchas amenazas, dando vueltas por la Web, protegerse, prevenirse y armarse para defender nuestra información resulta una tarea vital. Si bien antes era suficiente utilizar un simple antivirus, la veloz evolución y proliferación de nuevas amenazas hicieron que fuera necesario instalar otros softwares de protección en las computadoras.



SUITES DE SEGURIDAD

Entre las soluciones posibles sin dudas las más completas son las Suites de Seguridad, también conocidas como Internet Security Suite. Se trata de conjuntos de aplicaciones que generalmente reúnen antivirus, firewall, antiphishing, antispyware y herramientas de protección para el correo electrónico basura. Además de otorgar la posibilidad de incorporar funciones de control para que los padres protejan a sus hijos en Internet, y la posibilidad de realizar copias de seguridad automáticas para compensar eventuales pérdidas de datos.

Existe una gran variedad de fabricantes, versiones, funcionalidades, precios y ofertas por lo que resulta sumamente difícil confeccionar un ranking o elegir a unos sobre otros. Porque además depende de las necesidades de cada caso particular que una solución va a resultar más efectiva que otra. Por eso elegimos las suites más populares y completas del mercado, las probamos en nuestro laboratorio y les contamos absolutamente todo sobre su rendimiento, qué aplicaciones ofrecen y cuáles no, para ofrecerle la posibilidad de elegir cual es la opción que mejor se ajusta a sus necesidades.

El principal objetivo de las suites de seguridad es proteger los equipos sin que el usuario tenga la necesidad de adquirir conocimientos especiales sobre el tema. Apuntan básicamente a hogares o pequeñas y medianas redes de empresas. Por lo tanto sus aplicaciones deben poder integrarse de la manera más efectiva posible y su manejo debe ser sencillo, como para que cualquier usuario promedio pueda utilizarla sin problemas.

Por lo general las suites basan el núcleo de su funcionamiento en el sistema antivirus, sin embargo cada vez toman más importancia los firewalls ya que se constituyen en la primera línea de defensa y permiten evitar el peligro incluso antes de que el sistema antivirus o antispyware tengan que intervenir. Hoy en día también son muy importantes los sistemas antispam, no obstante, por lo general la mayoría de las suites no cuentan aún con sistemas muy elaborados ya que no poseen algoritmos de detección muy precisos y se apoyan generalmente en la actividad del usuario para generar sus propios patrones de descarte de correo. La protección contra el spam es uno de los campos a mejorar.

Entre las principales suites presentadas este año, se destacan aquellas que han empezado a ofrecer además sistemas de protección para trabajar en red y también la posibilidad de realizar copias de seguridad y sobre todo proteger la información personal como claves y datos bancarios.



MICROSOFT WINDOWS LIVE ONECARE 2.0

Para contar con esta suite es necesario suscribirse a **OneCare**, lo que asociado a una identidad Live ID, del MSN o Hotmail, permite instalar este sistema en hasta tres máquinas.
Esta suite lógicamente utiliza la ventaja de tener una gran integración con el sistema operativo Windows por lo que puede realizar tareas como la gestión de impresoras en red de manera automática, o gestionar de manera segura las conexiones inalámbricas con funciones como la configuración automática del router inalámbrico o la activación de la encriptación para PC. Sin embargo esa ventaja termina convirtiéndose en un riesgo en algunos casos. Así por ejemplo la suite trabaja siempre con encriptación WEP, para facilitar la conexión con todo tipo de productos ya que WEP es uno de los protocolos más extendidos, en lugar de los más efectivos WPA o WPA2, lo que limita la seguridad. Además de contar con las prestaciones básicas de una suite, el OneCare trae la opción de copia de seguridad. El software es muy intuitivo y fácil de manejar. OneCare es bueno detectando malware, aunque mostró grandes problemas para detectar los keylogger, y su firewall aunque se mostró invulnerable ante ataques de malware, resultó relativamente fácil de desactivar. Aunque hay que reconocerle que una vez desactivado siguió protegiendo la mayoría de los puertos. Por otro lado la suite OneCare resulta bastante lenta en cuanto a la actualización de nuevas amenazas sobre todo si la comparamos con los líderes del mercado. La suite Microsoft Windows Live OneCare 2.0, puede ser una buena opción para aquellos que buscan una suite de bajo costo y fácil de usar, sobre todo aquellos que no quieren tener que trabajar mucho en la configuración del software. No se comercializa en Argentina.

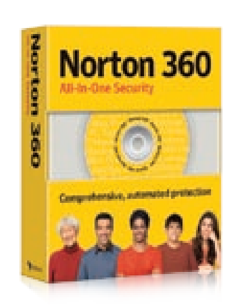
HTTP://ONECARE.LIVE.COM/



KASPERSKY INTERNET SECURITY 7.0

El **Internet Security 7.0 de Kaspersky** combina una interfaz de primera clase con un desempeño sólido en la detección de amenazas.
Kaspersky produjo buenos resultados en la mayoría de las pruebas de detección y desinfección de programas maliciosos. Hizo un arduo trabajo en la búsqueda de amenazas ocultas en archivos comprimidos y en todos los tipos de tráfico de correo electrónico y produjo la respuesta más rápida a los brotes de nuevos malware, ya que suministró firmas actualizadas en un período de 2 horas.
El programa de Kaspersky resultó excelente detectando gusanos de correo electrónico, pero su velocidad de exploración no es de las mejores. Por su parte, el sistema de protección de datos es excelente ya que nos advierte cuándo otros programas intentan acceder o enviar datos desde un área de almacenamiento protegida, ayudando a cuidar datos clave como los números de tarjeta de crédito; mientras que el firewall protege todos los puertos haciendo que la máquina sea invisible ante ataques externos. La interfaz intuitiva del conjunto de aplicaciones se destaca del resto, cuando termina una exploración, recibe un informe presentado con pestañas para separar el contenido que incluso identifica las configuraciones usadas durante la exploración. Sin embargo esta suite necesita muchas configuraciones por parte del usuario por lo que puede resultar un tanto incómoda para aquellos con pocas nociones de seguridad. En caso contrario y realizando las configuraciones necesarias el Kaspersky ofrece una protección extraordinaria que solo unos pocos pueden ofrecer, ya que sus sistemas antivirus, antispyware y su firewall, es decir el corazón de las suites de seguridad, son de las mejores del mercado.

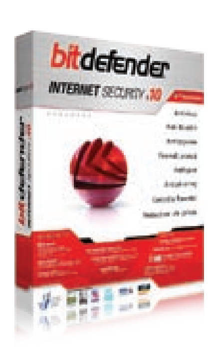
HTTP://WWW.KASPERSKY.COM/

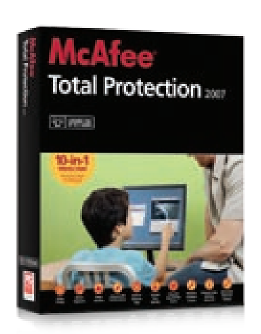


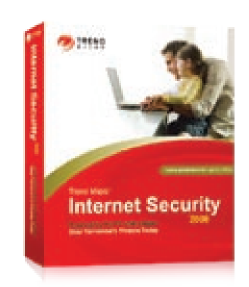
SYMANTEC NORTON INTERNET SECURITY 2008

El conjunto de aplicaciones **Norton** es desde hace unos años una de las más prestigiosas y reconocidas del mercado y en varias de las pruebas demostró el porqué. Es fácil de usar, viene con una gran cantidad de extras y es muy eficaz en la exploración. En cuanto a la erradicación de infecciones su desempeño es excelente, en especial en el combate contra rootkits, activos e inactivos. La versión 2008 trae nuevas aplicaciones como tecnología BrowserDefender que ayuda a mejorar la seguridad en la Web y un sistema de gestión de instalaciones en red, el Network Map, que facilita la monitorización de la seguridad de todas las máquinas sin la necesidad de trasladarse físicamente hacia ellas. El antispam y el control parental se pueden instalar opcionalmente pero este es un punto a mejorar.
El firewall es uno de los mejores que vimos ya que bloqueó todos los ataques masivos y resulta prácticamente imposible de desactivar. En cuanto a los ataques basados en exploits, la suite mostró un desempeño perfecto utilizando su sistema Intrusion Prevention System, un excelente servicio ante estos ataques cada vez más extendidos. El nuevo sistema de protección de identidad, Identidy Safe, hace un gran trabajo de gestión de información personal y contraseñas. La interfaz está bien distribuida y las alertas de detección emergentes por lo general son comprensibles. Norton Internet Security 2008 rankea alto entra las mejores suites del mercado ya que resulta una verdadera garantía para proteger nuestras computadoras además de ser muy intuitivo y necesitar una mínima participación del usuario para desactivar las amenazas y obtener el máximo rendimiento. Si bien aún puede mejorar los sistemas antispam y el control de padres, ofrece una garantía de seguridad completa.

HTTP://WWW.SYMANTEC.COM/INDEX.JSP







Bitdefender Internet Security 2008

Esta suite además de estar provista de los esenciales antivirus, antispyware y firewall cuenta con protección antispam y control parental. Esta versión incluye también un módulo de copia de seguridad. La interfaz es excelente, muy intuitiva, incluso para quienes nunca han utilizado un programa antivirus. Quizás una de sus mayores virtudes sea la excelente integración entre antivirus y antispyware además de su excelente desempeño detectando malware. El firewall de **Bitdefender** es efectivo ocultando la PC contra los sondeos externos. Quizás uno de los debes sea que la interfaz resulta un poco complicada para los usuarios. En cuanto a las pruebas heurísticas mostró un gran desempaño enfrentando malware desconocido, pero no se mostró tan eficiente limpiando infecciones. En líneas generales Bitdefender Internet Security 2008 parece tener las herramientas necesarias para cumplir con su promesa de garantizar cada uno de los bits. La licencia abarca tres instalaciones durante dos años.

HTTP://WWW.BITDEFENDER.COM/WORLD/

Mc Afee Total Protection 2008

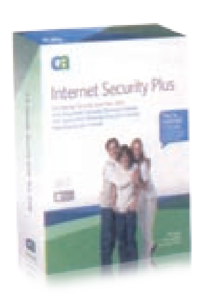
La **McAfee Total Protection 2008** es la suite que más prestaciones ofrece de todas las analizadas pero su firewall y antispyware no son de los más sólidos. La versión 2008 no se diferencia mucho de la anterior, aunque presenta algunas mejoras en especial una interfaz más intuitiva y mejor diseñada. Cuenta con antivirus, antiphishing, antispyware, firewall, la posibilidad de backup, algo que otras suites no ofrecen y protección para 3 equipos. El antispam funciona de manera óptima al igual que el sistema contra programas malware, pero no así su firewall que logró ser penetrado y desactivado además de un control parental deficiente y un sistema antipornografía bastante irregular. Como positivo se puede decir que es una de las suites más fáciles y accesibles para utilizar por usuarios con poco conocimiento de seguridad. Ofrece más aplicaciones que el resto por ejemplo la posibilidad de realizar backup de nuestra información pero podría ofrecer un mayor nivel de seguridad, en especial en lo que respecta al firewall. Sin embargo si se tiene en cuenta la relación costo beneficio, se trata de un producto muy competitivo.

HTTP://WWW.MCAFEE.COM

Trend Micro Internet Security 2008 Pro

La Suite **Trend Micro Internet Security 2008 Pro** ofrece una licencia para proteger hasta 3 equipos, una amplia protección y el programa se instala fácil y muy rápido. Esta suite además de las características estándar, ofrece algunos extras, como sistema antiphishing. La instalación no resulta de las más sencillas pero suma puntos con excelente bloqueo del malware además de un excelente filtrado del spam y la posibilidad de gestionar remotamente otras instalaciones. Presenta algunos problemas con la interfaz, pero esta suite es una de las más efectivas en tareas de limpieza de infecciones y es una de las más veloces. El sistema de control parental como en casi todas las suites analizadas no es de los más efectivos. Sin dudas la versión 2008 ha mejorado notablemente con respecto a versiones anteriores: el firewall por ejemplo detuvo todas las amenazas que se presentaron pero lanzando una gran cantidad de avisos que pueden ser molestos. La Trend Micro Internet Security 2008 Pro ofrece una buena garantía de seguridad, ya que se destaca en aquellos puntos clave que toda suite de seguridad que se precie debe ofrecer.

HTTP://US.TRENDMICRO.COM/US/PRODUCTS/PERSONAL/



CA Internet Security Suite Plus 2008

La nueva versión de **CA Internet Security Suite Plus 2008** ofrece muchas novedades y mejoras desde la versión presentada el año pasado. Por ejemplo la versión 2008 incluye un inspector Web para identificar sitios fraudulentos y la interfaz está dividida en siete módulos intentando hacer que la experiencia del usuario sea más agradable y sobre todo intuitiva. Sin embargo esta solución integral de seguridad no ofrece un buen firewall ya que el ZoneAlarm utilizado en la versión anterior fue reemplazado este año por el Tiny Personal Firewall con un resultado negativo. Este firewall resulta vulnerable cuando recibe ataques masivos de malware y su interfaz requiere una constante interacción por parte del usuario. Por ejemplo cada vez que una nueva aplicación intenta acceder a Internet es bloqueada y solo el usuario puede permitirle ingresar a la red. Esto termina resultando molesto si se lo compara con otras suites que apoyándose en su base de datos realizan estas tareas de manera independiente. El antivirus es en general efectivo y el antispyware ha mejorado mucho desde su anterior versión. El antispam por su parte comienza siendo muy simple ya que simplemente envía a cuarentena todos los correos provenientes de direcciones desconocidas, pero es capaz de mejorar basándose en la gestión que realiza de su correo el usuario. Si bien la suite deberá mejorar el firewall, posee una interfaz muy agradable para el usuario, quizás la más intuitiva y fácil de utilizar de todas y no falla en dos de los puntos clave de las herramientas de seguridad, el antivirus y el antispyware.

HTTP://SHOP.CA.COM/MALWARE/INTERNET_SECURITY_SUITE.ASPX



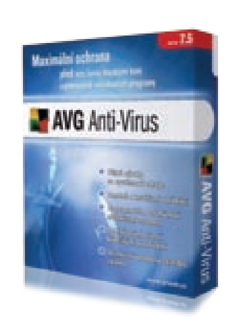
Eset Smart Security 3.0

La **Eset Smart Security 3.0** es una de las más atractivas y completas suites del mercado. Se destaca especialmente por una gran integración entre sus componentes, una de las cuestiones más difíciles e importantes de lograr por una suite. Este año además presenta varias novedades como una nueva interfaz y mejoras en el escaneo.

Esta suite, como su nombre lo indica, realiza la mayoría de sus tares de forma automática y sin que el usuario lo note. Así actualiza las amenazas, escanea el sistema de archivos y detecta y elimina ataques por la red y archivos peligrosos. Si el usuario lo prefiere también posee la opción de participar activamente y elegir qué hacer en cada caso o configurar previamente cómo quiere que actúe el sistema.

La velocidad y la eficaz detección son sus marcas registradas sin embargo presenta algunos falencias. Por ejemplo carece de sistema de control parental, las herramientas de copia de seguridad, protección de la identidad y una licencia multi-usuario, cosas que otras suites ofrecen. Pero por otro lado parece suplir esas carencias con un gran desempeño en los núcleos centrales de una solución de seguridad, es decir, excelente protección contra virus, spyware, spam y un sólido firewall. Otro de los puntos que la destacan es que necesita mínimos requisitos y espacio para funcionar. Además de una interfaz sumamente limpia y ordenada que parece ideal para el ámbito profesional.

HTTP://WWW.ESET.COM/SMARTSECURITY/INDEX.PHP



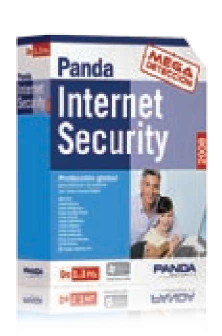
AVG Internet Security Home 7.5

AVG ganó reputación mundial gracias a que su AVG Anti-Virus Free Edition 7.5 es uno de los más efectivos antivirus gratuitos del mercado. Sin embargo para quienes necesitan una protección integral AVG ha desarrollado la suite Internet Security Home 7.5. Esta es una de las suites más nuevas del mercado ya que fue lanzada hace apenas un año, por lo que aún le falta desarrollarse en algunos aspectos, pero por la historia de los antivirus AVG y por los resultados obtenidos por la suite en tan poco tiempo merece tener el crédito abierto.

En las pruebas esta suite se mostró muy eficaz eliminando spyware, sin embargo el firewall requiere la interacción constante del usuario mediante cuadros de diálogo del sistema operativo y carece de protección ante el malware que intenta evadir el funcionamiento normal del mismo. En cuanto al spam el sistema se mostró realmente efectivo eliminando la gran mayoría de los correos basura, sin afectar ningún correo válido, un resultado superior a muchas de las demás suites.

AVG Internet Security 7.5 es una interesante propuesta ya que posee un excelente antivirus y su sistema antispam es uno de los más efectivos que se pueden encontrar en el mercado, sin embargo su firewall le resta puntos a un buen sistema que si puede mejorar estas fallas se convertirá en una de las suites más completas del mercado, al nivel de las más renombradas y costosas.

HTTP://WWW.GRISOFT.COM/WW.HOMEPAGE



PANDA INTERNET SECURITY 2008

Panda se ha ganado un respetable nombre en el mundo de la seguridad en base a que sus productos siempre se encuentran entre los más destacados y por ello uno siempre espera y pide más de sus lanzamientos. La suite Panda Internet Security 2008 resultó la más eficaz detectando y eliminando virus y spyware, en estos fundamentales aspectos la suite se muestra invulnerable. Además de contar también con un sólido firewall, que difícilmente pueda ser desactivado. Sin embargo la versión 2008 no presenta grandes novedades o mejoras con respecto a anteriores versiones y el sistema antispam no respondió a la altura de lo que se espera de un producto Panda. Y otra de las contras de esta suite es que necesita mucho espacio en el disco para funcionar, por lo menos 500 MB disponibles. Entre las pocas novedades que trae esta versión la seguridad WiFi y la posibilidad de realizar copias de seguridad son las más destacadas.

En cuanto a las nuevas amenazas, la suite ofrece un excelente desempeño basándose en el sistema TruPrevent, lo que le permite identificar cada uno de los nuevos peligros que dan vueltas por la Web. Además el sistema Panda Identity Protect se encarga de asegurar toda la información personal en la red. Sin embargo la velocidad de trabajo no es la ideal, ya que utiliza muchos recursos físicos de la PC. También se deberá mejorar el sistema de control para padres, el antispam y el sistema de copia de seguridad. No obstante su antispyware es realmente uno de los mejores del mercado, y también se destacan su firewall y su antivirus por lo que la suite garantiza una óptima y total protección.

HTTP://WWW.PANDASECURITY.COM/ARGENTINA/

Glosario

PHISHING

Es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

SPYWARE

Los programas espías o spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

FIREWALL

Es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. En general se utilizan entre la red local e Internet como dispositivo de seguridad que evitar que los intrusos puedan acceder a información confidencial.

ROOTKIT

Es una herramienta o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder a otros programas, procesos, archivos, directorios, llaves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos.

MALWARE

Es un software que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.

SPAM



Se llama spam o correo basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor.

Tabla de características

Fabricante / Modelo	AVG Antivirus Internet Security Home 7.5	Bitdefender Internet Security 2008	CA Internet Security Suite Plus 2008	Kapersky Internet Security 7.0	Eset Smart Security
Número de licencias	3	1	3	1	1
Duración de la licencia (años)	1	de 1 a 3	1	1	1
Aplicaciones Integradas					
Antivirus	Sí	Sí	Sí	Sí	Sí
Firewall	Sí	Sí	Sí	Sí	Sí
Anti-Spam	Sí	Sí	Sí	Sí	Sí
Anti-Spyware	Sí	Sí	Sí	Sí	Sí
Anti-Phising	Sí	Sí	Sí	Sí	No
Protección de datos personales	No	Sí	No	Sí	No
Control parental	No	Sí	Sí	Sí	Sí
Control de redes domésticas	No	No	No	No	Sí
Detención Wi-Fi	No	No	No	No	Sí
Actualización automática	Sí	Sí	Sí	Sí	Sí
Detección heurística	Sí	Sí	Sí	Sí	Sí
Backup	No	Sí	Sí	No	No
Disco de rescate	No	No	No	Sí	No
Configuración del Sistema	No	No	No	No	No
Requisitos Mínimos					
Procesador	Pentium 300 MHz o sup	Pentium 800 MHz o sup	Pentium 300 MHz o sup	Pentium 300 MHz o sup	Pentium 400 MHz o sup
Memoria RAM	256 MB	512 MB	256 MB	128 MB	128 MB
Espacio Libre en el disco duro	No Disponible	60 MB	No Disponible	50 MB	35 MB
Disponible para Windows	2000, XP y Vista	2000, XP y Vista	2000, XP y Vista	2000, XP y Vista	2000, XP y Vista

MacAfee Internet Security Suite 2008	Norton Intenet Security 2008	Microsoft Windows Live OneCare 2.0	Panda Security Internet Security 2008	Trend Micro Internet Security 2008
3	3	3	3	3
2	1	1	1	1
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	No
Sí	Sí	Sí	Sí	Sí
No	Sí	Sí	No	Sí
No	No	Sí	No	Sí
Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	Sí
No	No	Sí	Sí	No
No	No	No	No	No
Sí	No	Sí	No	No
Pentium 500 MHz o sup	Pentium 300 MHz o sup	Pentium 300 MHz o sup	Pentium 300 MHz o sup	Pentium 350 MHz o sup
256 MB	256 MB	256 MB	128 MB	256 MB
No Disponible	350 MB	600 MB	270 MB	300 MB
2000, XP y Vista	XP y Vista	XP y Vista	2000 y XP	XP y Vista

TECNOLOGÍAS DE SEGURIDAD EN WINDOWS VISTA

Autor: Chema Alonso

Parece que fue ayer cuando Microsoft tomó conciencia de la importancia de la seguridad y ya han pasado casi 6 años desde el comienzo de la Trustworthy Computing Initiative (TCI) o para los hispanoparlantes la "Iniciativa de Informática de Confianza". Decidirse a arrancar esta iniciativa no fue algo tomado a la ligera.

Los productos de Microsoft, hasta aquel entonces diseñados para "instalar y listo!" habían sido objetivo de la comunidad de investigadores de seguridad, haciendo de ellos un foco de exploits y lo aún más importante y peligroso, virus y troyanos.

Trustworthy Computing Initiative (TCI)

La compañía comenzó esta iniciativa, con una mira de 10 años de duración, contrató a algunos de los mejores gurús de la seguridad informática para que se aremangaran y condujeran la fábrica de software de Redmond en un equipo concienciado, formado y preparado para afrontar la puesta en el mercado de productos software seguros... o al menos, mucho más seguros.

Michael Howard, Mark Russinovich posteriormente o el reciente Crispin Cowan han sido algunos de los nombres propios que han entrado a formar parte de los expertos de seguridad con los que cuenta la empresa de la banderita de colores para lograr esta labor.

El primer producto que se vio de lleno en la TCI no fue Windows XP, éste había sido concebido y liberado tiempo antes, así que lo primero que se hizo fue sacar una lista de Service Packs para los principales productos. Estos Service Packs habían sido diseñados y concebidos dentro de la TCI pero los productos no habían sido diseñados dentro de la TCI. Así, Windows XP SP2 reforzó considerablemente el sistema Windows, pero no se pudo tocar la arquitectura desde abajo.

Como muchos ya sabréis, el primer sistema operativo diseñado dentro de la TCI no es otro que aquel que tuvo como nombre código "Longhorn", es decir, nuestro amigo Windows Vista. En él, se aplicaron las tecnologías de seguridad que estaban incluidas en Windows XP SP2 junto con una nueva arquitectura para dotar al sistema operativo de los mecanismos necesarios para protegerse frente a amenazas futuras.



DEP y ASLR

Cuando un procedimiento es invocado en el sistema operativo, lo primero que se hace es situar en la pila del sistema la dirección de retorno a la que debe volverse cuando el procedimiento se termine de ejecutar. Encima de ese valor se apilan los parámetros que necesita para su ejecución el procedimiento. Si no se comprueba el tamaño de los parámetros que van a ser apilados, un atacante podría introducir un dato de mayor tamaño del que tiene reservado y sobrescribir el valor de retorno del contador de programa. De esta manera conseguiría el control de la ejecución. Para hacerlo más "divertido" el atacante puede introducir un programa en los parámetros y después hacer que la dirección de retorno apunte a su programa. Haciendo esto el atacante consigue ejecutar un programa en el sistema.

Para evitar esto existen diversas tecnologías, pero las más importantes son DEP (Data Execution Prevention) y ASLR (Address Space Layout Randomization). La tecnología DEP se puede aplicar por software o por hardware en Windows Vista. Cuando se aplica DEP por hardware el sistema toma ventaja de la tecnología NX incorporada en los microprocesadores hace ya varios años. Los microprocesadores marcan zonas de memoria como de programa (eXecution) o de datos (NoneXecution). De esta forma el sistema operativo no ejecuta ningún programa almacenado en una zona de memoria destinada a datos, o lo que es lo mismo, ninguna dirección del contador de programa puede apuntar a una zona de datos. De esta forma se previene la inyección de programas en desbordamiento de datos.

No obstante, esta tecnología no evita completamente estos ataques pues el atacante podría hacer que se ejecute un programa del sistema que le permitiera tomar control de la máquina. Para evitar esto, se utiliza la tecnología ASLR. Hasta Windows XP, cuando el sistema operativo arranca una librería del sistema, ésta es cargada siempre en la misma dirección de memoria.

Al usarse siempre la misma dirección, los atacantes pueden crear sus programas para apuntar a direcciones de librerías internas conocidas. Para evitar esto la tecnología ASLR permite que un determinado programa sea cargado cada vez en una ubicación distinta de la memoria dentro de un rango de 256 posibles valores. De esta forma un exploit tendría 1 posibilidad entre 256 intentos de acertar con la llamada correcta.

Como protección adicional, DEP en Windows Vista, tiene una versión basada solo en software que vino ya en XP SP2 y cuyo objetivo es garantizar la integridad de las funciones que son



invocadas en el tratamiento de los mensajes de excepción que deben ser gestionados por el sistema operativo. Para ello se comprueba la integridad de los binarios del sistema que se encargan del tratamiento de los mensajes de error antes de entregarles el control.

Bitlocker

Otro de los vectores de ataque en las empresas ha sido el robo de ordenadores portátiles o el arranque en paralelo del sistema. Es decir, llegar a un equipo, arrancarlo con otro sistema y acceder a todos los datos que posea. Para evitar esto se utilizan, desde hace tiempo, sistemas de cifrado de disco. Windows Vista y Windows Server 2008 vienen acompañados de una tecnología que permite cifrar todo el volumen del disco llamada Bitlocker.

Toda la información del disco es cifrada con una clave llamada Full Volume Encryption Key (FVEK). Para poder acceder a los datos, es decir, para que se pueda tan siquiera reconocer la estructura del sistema de ficheros es necesario conseguir la FVEK. Esta clave está almacenada en los metadatos del volumen pero cifrada con otra clave, llamada Volume Master Key (VMK).

Cómo conseguir la VMK para poder descifrar la FVEK y poder acceder a los datos es el corazón de la seguridad del sistema. Para protegerla y garantizar un arranque seguro, esta clave es cifrada por uno o varios "protectores de clave" que pueden ser mantenidos en diferentes sitios. Se puede utilizar una memoria USB con la clave de descifrado de la VMK o almacenar en el Directorio Activo una clave que permita el acceso en caso de desastre o también utilizar el famoso chip TPM (Trusted Platform Module) para conseguir tener la clave (ver figura 1).

Chip TPM (Trusted Platform Module)

¿Qué es el chip TPM? Es un chip incluido en los nuevos equipos portátiles con capacidades de almacenamiento criptográfico que permite almacenar claves de forma segura y comprobar que el equipo que está siendo arrancado no ha sido modificado, es decir, que el disco duro, por ejemplo, no ha sido cambiado a otro hardware.

Otra pregunta que podemos realizarnos es si es posible utilizar la tecnología Bitlocker si el equipo no tiene chip TPM. La respuesta es por supuesto que sí. El chip TPM se puede utilizar para almacenar las claves de Bitlocker, pero estas pueden ser almacenadas de otra forma, como por ejemplo en una memoria USB. Procura no llevar el ordenador y la memoria USB en la misma bolsa ya que entonces no va a servir de mucha protección.

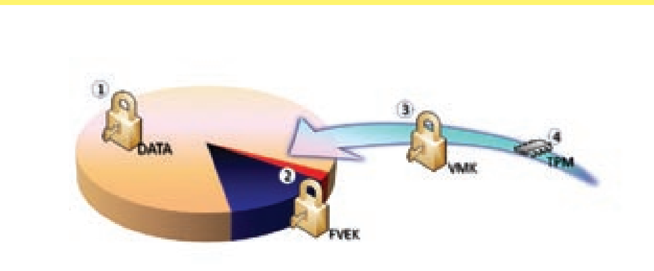


Fig. 1: Bitlocker y el Chip TPM

```
Windows BitLocker Drive Encryption Password Entry

Enter the recovery password for this drive.

   _____ _____ _____ _____
   _____ _____ _____ _____

Drive Label:
Password ID:

Use the function keys F1 - F9 for the digits 1 - 9. Use the F10 key for 0.
Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.

The UP and DOWN ARROW keys may be used to modify already entered digits.

  ENTER=Continue                                                ESC=Exit
```

Fig. 2: Clave de Recuperación en Bitlocker



Si la clave puede estar almacenada en otros sitios, la pregunta entonces es para qué es útil el chip TPM entonces. El almacenamiento de la clave de Bitlocker es sólo una de las funciones del chip, pero su principal función es garantizar el arranque seguro de la plataforma. En las conferencias Blackhat de 2006 se demostró que era posible crear un rootkit con las funciones de la BIOS, de tal forma que una vez arrancado el ordenador éste ya estaba comprometido. El chip TPM no arrancará el sistema y no descifrará la VMK si ha sido manipulada la plataforma. ¿Y si se rompe la placa no podré acceder a la información si tengo la clave en el chip TPM? Para esos entornos el sistema permite descifrar la información con una clave de recuperación. Ésta clave puede ser almacenada en el Directorio Activo junto con la información de la cuenta de la máquina, de tal forma que la empresa siempre pueda recuperar los datos. La tecnología Bitlocker y el chip TPM ayudan a proteger el equipo para conseguir un arranque seguro y confiable, pero si el equipo ya está arrancado el sistema de protección no recae sobre él. Es decir, si un portátil es arrancado y posteriormente suspendido temporalmente, el chip TPM ya ha liberado la clave y el disco está descifrado y por tanto, la seguridad de la plataforma recae en la seguridad que tenga el sistema para volver a ser despertado (ver figura 2).

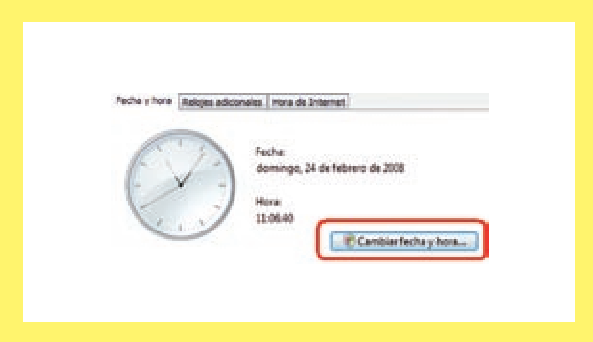


Fig. 3: Opciones que necesitan privilegios están marcadas con un icono especial

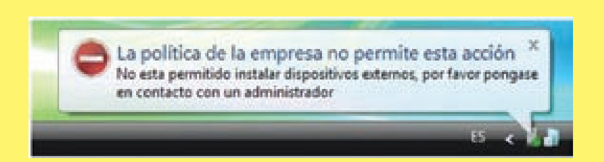


Figura 4: Directivas de Restricción de Instalación de dispositivos

A finales de febrero de 2007 un grupo de investigadores de seguridad ha publicado un documento en el que dicen haber conseguido saltarse estas protecciones si el sistema está suspendido. Imaginemos que un usuario está trabajando y en lugar de apagar el equipo simplemente suspende su portátil. En esta situación el sistema ya ha sido arrancado y la clave de cifrado ha sido liberada. Para poder acceder al equipo hay que conseguir la contraseña de bloqueo que está en memoria. Lo que proponen realizar es bajar la temperatura de la memoria RAM a - 50 grados Celsius. A esta temperatura la memoria se congela y puede ser desenchufada del equipo e incrustada en un equipo que permita analizar su contenido. Una vez analizado, y extraída la información de la clave, la memoria es devuelta al ordenador original y se despierta el equipo. Curioso cuanto menos.

User Account Control (UAC)

Uno de los problemas de seguridad que tenía Windows XP es la necesidad de usar cuentas privilegiadas para poder realizar algunas de las tareas que para muchos de nosotros son normales. Enchufar una cámara o un escáner USB, conectarse a una red inalámbrica o cambiar la dirección IP de una tarjeta de red son acciones que implican cambios en la configuración del sistema operativo y, por lo tanto, deben ser hechas por usuarios privilegiados. Este hecho ha llevado a que gran parte de los usuarios utilicen su ordenador con cuentas de administradores del sistema por simple comodidad.

Si la cuenta que se está utilizando es de administración también tendrá los mismos privilegios todo programa ejecutado por ella. Así, cuando se arranca un navegador para conectarse a Internet este lleva asociados los privilegios de la cuenta. Si la seguridad del programa fuera comprometida por un ataque entonces quedarían expuestos los privilegios de administración del sistema, como ha sucedido muchas veces.

Para evitar esta situación en Windows XP SP2 se recomendaba la opción de “Ejecutar como”. Esta solución es una solución “de más a menos”. Es decir, se trabaja por defecto como administrador y cuando se va a ejecutar determinados programas se elige otra cuenta del sistema con menos privilegios. En Windows Vista se ha cambiado el enfoque y ahora, aunque un usuario tenga privilegios de administración, estos no son utilizados por defecto, quedando relegado a ser un usuario no privilegiado.

En el caso de que el sistema requiera estos privilegios se solicitará al usuario “EXPLICITAMENTE” el uso de estos mediante un cuadro de dialogo bloqueante que informa detalladamente cuál va a ser el uso que se va a dar a esos privilegios. Ahora bien, si un troyano pide privilegios y el usuario se los concede entonces no hay protección que valga (ver figura 3).

Control de dispositivos USB

Con el avance de las tecnologías van apareciendo nuevas amenazas y hoy en día, en una memoria USB o en un disco duro USB puede caber toda la información confidencial de una empresa. La fuga de información mediante el uso de dispositivos USB ha sido un quebradero de cabeza de muchas compañías. Las empresas implementan firewalls, sistemas de detección de Intrusos, sistemas de prevención de ataques y mecanismos de cifrado para que al final un usuario con permisos enchufe

su disco duro de 40 Gb de capacidad de almacenamiento y vuelque toda la información de la empresa y se la lleve a su casa, la cuelgue en Internet o la utilice en contra de los intereses de la empresa. Evitar esto ha sido tarea difícil y en Windows XP SP2 no había ninguna opción que permitiera controlar los dispositivos USB que se permitían conectar o no. En muchas empresas se ha llegado a deshabilitar el uso de conexiones USB en la BIOS. Con Windows Vista se puede gestionar qué dispositivos USB están permitidos y denegar el uso de otros. Esto le permite a las empresas y usuarios trabajar con cualquier dispositivo autorizado y que nunca nadie pudiera enchufar una memoria USB no autorizada (ver figura 4).

Dentro de las más de 800 directivas de seguridad en Windows Vista hay un conjunto de ellas pensadas especialmente para esta situación y, cuando se intente conectar un dispositivo no autorizado el sistema avisará de esta situación (ver figura 5).

MIC, UIPI y el modo protegido de IE7

En Windows Vista, el sistema ha sido segmentado por niveles de seguridad. Esto quiere decir que alguien que está en un nivel inferior de seguridad no va a poder hablar con un nivel más alto en la escala de seguridad. Para ello se utilizan dos tecnologías: Mandatory Integrity Control (MIC) y User Interface Privilege Isolation (UIPI).

MIC divide todos los datos del sistema en 5 niveles de seguridad que van desde el 0 (o anónimo) hasta el 400 (sistema). Ningún programa va a poder acceder a datos o ficheros situados en un nivel de integridad más alto. UIPI funciona de forma similar pero centrada en el intercambio de mensajes entre aplicaciones gráficas. En este caso ninguna aplicación gráfica va a poder enviar un mensaje a otra aplicación gráfica situada en un nivel superior y, por lo tanto, tampoco interceptar mensajes de otras aplicaciones. Como se puede ver en la figura 6, cada proceso en ejecución tiene un nivel de Integridad distinto. Es importante fijarse en que Internet Explorer está compuesto por dos procesos, uno de ellos es el que se expone a Internet (iexplore) que corre con nivel de integridad bajo y otro, que es la representación en el sistema y el que tiene los privilegios de la cuenta (ieuser) que se ejecuta con nivel de integridad medio. En el caso de que un exploit ataque a Internet Explorer

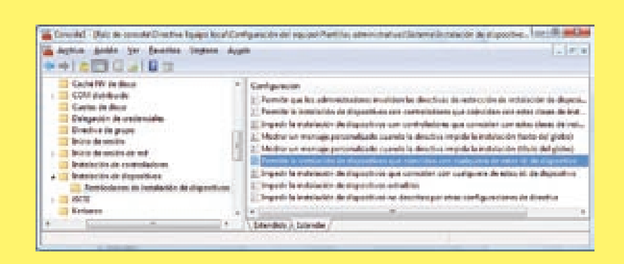


Figura 5: Dispositivo USB no permitido



7 sobre Windows Vista, sólo lograría obtener privilegios de nivel de integridad bajo, protegiendo así todo el resto del sistema. Esta arquitectura es el modo protegido de Internet Explorer 7. Más (y muchas más) fortificaciones de seguridad Windows Vista ha sido pensado desde el principio con la seguridad como requisito básico, así que las novedades de seguridad son muchas. De forma más rápida algunas otras son:

Firmado de Drivers

Siempre pensando en proteger el sistema contra los más evolucionados programas de malware y también para conseguir una mayor estabilidad, Microsoft ha obligado a las compañías que deseen desarrollar drivers para Windows Vista en versiones de 64 bits, que estos deban ir firmados digitalmente.

Esto ayuda a mantener una calidad en el desarrollo de los drivers y a que no se pueda introducir en el kernel del sistema ningún programa nocivo sin conocer su procedencia.

Integridad de código

Todo el código del sistema operativo viene firmado y comprobada su integridad, es decir, antes de que se ejecute una librería o componente del sistema se comprueba la integridad del fichero para saber si es el original o ha sido cambiado. Para ello en Windows Vista y Windows Server 2008 se mantiene un catalogo de firmas con todos los componentes del sistema y estos son revisados antes de ejecutar el programa.

Windows Service Hardening (WSH)

Los servicios en la plataforma Windows han sido uno de los elementos más atacados. Esto se debe a que se están ejecutando continuamente y con una cuenta del sistema. En Windows Vista se han realizado una serie de cambios importantes. En primer lugar se ha aislado de cualquier sesión de usuario, es decir, los servicios se ejecutan en la sesión 0 y el primer usuario en la sesión 1, con lo cual no interactúan directamente. Además los servicios cuentan con una optimización de privilegios para que el uso de credenciales que haga sea el menor posible, reduciendo así la superficie de exposición. Al mismo tiempo se ha dotado a cada servicio de un SID para que puedan ser controlados sus accesos mediante listas de control de acceso y se ha añadido un manifiesto a cada uno que autolimita lo que puede o no puede hacer cada servicio.

Lógicamente, la idea de toda esta fortificación es reducir los riesgos en caso de que un servicio quedara comprometido.

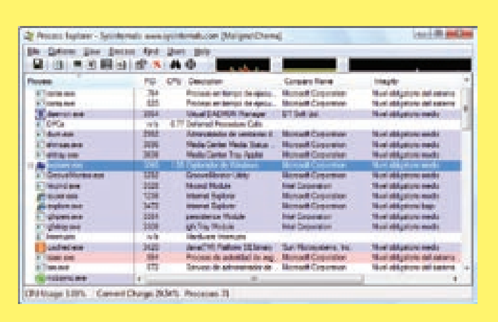


Figura 6: Niveles de Integridad vistos con Process Explorer

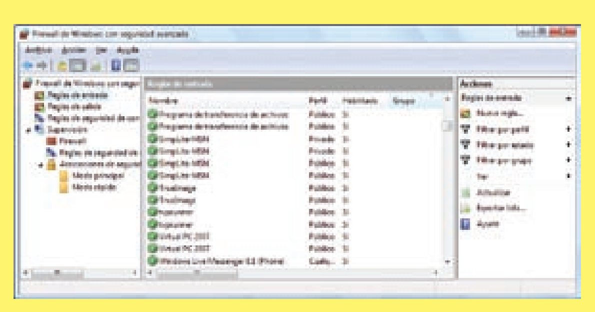


Figura 7: Firewall de Windows Vista

Nuevo Firewall e IPSEC

El nuevo firewall que acompaña a Windows Vista poco tiene que ver con el antiguo “Internet Connection Firewall” que acompañaba las versiones de XP S2. En este caso es un firewall que se integra con IPSec y que permite configurar con todo lujo de detalles la configuración de seguridad de tu plataforma. Tiene la ventaja de trabajar con perfiles de conexión, es decir que dependiendo de la red a la que uno se conecte se podrá aplicar una u otra configuración de seguridad. Por defecto trae tres perfiles configurados para redes públicas, privadas y personales. En el firewall se pueden configurar reglas por programa, usuario, entrada/salida y las opciones de ipsec (ver figura 7).

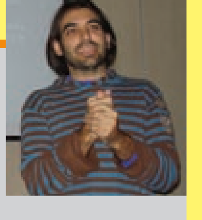
Windows Update y Windows Defender

Windows Update sigue estando presente en Windows Vista, pero además sigue ampliando la cantidad de componentes que se actualizan a través de él. En un principio el Windows Update sólo actualizaba los parches críticos del sistema, hoy en día se encarga también de actualizar el sistema completo e incluso componentes extendidos, como por ejemplo las firmas de Windows Defender (evolución de Microsoft Antispyware), el componente antispyware que viene gratuito y de serie en el sistema.

Despedida

Windows Vista ha sido creado desde cero pensando en seguridad y se ha conseguido que sea el sistema operativo que mejores resultados de seguridad ha conseguido en su primer año de vida. Las tecnologías de seguridad en Windows Vista son mucho más que las que se han podido tratar en este artículo y si te sirve de recomendación, si yo me dedicara a hacer malware para robarte tu dinero, preferiría que no tuvieras Windows Vista.

Acerca del Autor



Chema Alonso

Microsoft MVP Windows Seucurity. Es ingeniero Informático y trabaja como consultor de Seguridad en Informática 64. Ponente habitual en conferencias de seguridad y tecnologías Microsoft. http://elladodelmal.com

nuevos tiempos en las amenazas por la red

Autor: David Barroso
Director de Investigación de S21sec



La velocidad con la que evolucionan los riesgos de utilizar Internet es tan rápida que es prácticamente imposible pararse un momento a reflexionar y mirar hacia atrás: sólo es posible mirar hacia el futuro si no se quiere perder el equilibrio, y por supuesto, el control. Esta transformación tan frenética está presente en la Seguridad de la Información, área que es cada vez más importante en todas las organizaciones, por lo que se exige tener que adaptarse continuamente a las evoluciones de los peligros que acechan sin descanso: no hay vacaciones, horas de cierre o descansos; la presencia y uso de Internet por parte de una organización implica estar disponible (online) 24 horas al día, 365 días al año (y consecuentemente, proteger los activos de la organización en el mismo horario).

Existen diferentes factores a tener en cuenta, necesarios para las futuras decisiones que habrá que tomar: el primero de ellos, el origen de los ataques que se pueden sufrir; hace tiempo que terminó la "época romántica" en la que muchos de los ataques eran fruto de la curiosidad y de demostrar la valía de ciertos adolescentes. La realidad actual es bien distinta. Existen bandas de crimen organizado que utilizan todos los recursos y tecnologías presentes en Internet para garantizar su anonimato y cometer todo tipo de felonías: phishing, pharming, scam, clickfraud, worms, zero-day exploits, spam, ataques de denegación de servicio distribuidos (DDoS) y un largo etcétera de amenazas a las que todos somos vulnerables. El objetivo que subyace en la mayoría de los ataques es siempre un motivo económico, pero muchas veces también ya se intercalan motivos políticos o relacionados con el espionaje industrial.

Estas bandas organizadas, que se encuentran en ciertas áreas del mundo, pero muchas veces con presencia local en todos los países, utilizan a su antojo cualquier tecnología que les favorezca: programación de malware para el robo de información, balanceo de carga y alta disponibilidad en sus infraestructuras (como por ejemplo fast-flux), utilización de proxies inversos encadenados utilizando máquinas comprometidas para ocultar su centro neurálgico, o el uso de XML o AJAX en sus paneles de control para manejar todos sus recursos.

Aquí se nota uno de los factores de cambio que se ha comentado: la utilización, cada vez mayor de malware para el robo de información y la posterior utilización de las máquinas infectadas para otro tipo de delitos (DDoS, proxies, clickfraud, etcétera). Este factor provoca que casi toda las inversiones que se han hecho en seguridad perimetral (cortafuegos, detectores de intrusos, antivirus de correo, filtrado de contenido) pierdan gran parte de su eficiencia para prevenir estos nuevos ataques. Tanto esfuerzo en proteger el perímetro de una organización tuvo su éxito y ya son pocos los que se obstinan en romper estas protecciones. En cambio, ha aparecido un nuevo talón de Aquiles: el usuario, que al final siempre es el eslabón más débil. Porque ¿de qué nos sirve contar con cortafuegos, IDS, antivirus, filtrado de contenidos o tecnologías similares si un empleado se infecta con un código malicioso simplemente visitando una página con un exploit zero-day como el existente de Acrobat Reader en Febrero? Este código no es detectado por los antivirus y utiliza una conexión HTTP

normal para enviar los datos robados y recibir órdenes. De hecho, las propias casas antivirus reconocen que no son capaces de soportar la gran cantidad de códigos maliciosos que se generan todos los días, y muchas veces existe esa ventana de tiempo en la que aún teniendo el sistema operativo con todos los parches, los sistemas son vulnerables.

No bajar la guardia

Las protecciones en el perímetro por supuesto que son necesarias, pero también es fundamental añadir más capas centrándonos en otros puntos que antes estaban más descuidados. Durante 2007 en el Centro de Operaciones de Seguridad (SOC) de S21sec se detectaron y remediaron más de 1.600 casos de fraude afectando a nuestros clientes; casi un 100 por ciento más que en el año anterior; este dato es tan sólo la punta del iceberg, puesto que realmente la cantidad de amenazas con las que nos enfrentamos crece de forma exponencial. ¿Cuántos intentos de intrusión se reciben todos los años? ¿Cuántas fugas de información no se detectan? ¿Cuántas páginas que se visitan intentan infectarnos? ¿Cuántas veces las redes inalámbricas son atacadas? ¿Cuántos dispositivos externos no fiables se conectan a computadoras corporativas o se conectan a redes públicas (aeropuertos, congresos, etcétera) o de no confianza? ¿Las computadoras corporativas tienen el disco duro cifrado en caso de pérdida o robo? ¿Y los backups de las computadoras?

Todas estas preguntas son simplemente un ejemplo de todos los riesgos que se sufren día a día y que forman parte del escenario. La seguridad al 100 por ciento no existe; sin embargo, todas las acciones que ponemos en práctica, por pequeñas que sean, permiten minimizar el riesgo frente a todas las amenazas. Es vital disponer de un asesoramiento experto en todas las áreas que pudieran ser afectadas por estos riesgos. Si no es posible, se debe contar con profesionales capacitados acostumbrados a no perder este rápido tren de evolución continua, o bien delegar a empresas especializadas en seguridad la gestión del ciclo de vida completo de la Seguridad de la Información: desde servicios de seguridad gestionada (MSS), controlando y monitorizando qué está pasando en una organización, hasta la ayuda para el cumplimiento de todas las normativas y estándares necesarios para el correcto y seguro funcionamiento de todas las áreas de negocio.

Virtualización

Actualmente los esfuerzos no sólo se están centrando en controlar quién se conecta a una red corporativa y cómo (muchos fabricantes tienen soluciones de control de acceso a la red como NAC o NAP). También se está extendiendo el uso de tecnologías de virtualización con diferentes objetivos, ya sea ahorro de costes o facilidad en su despliegue. La adopción de una nueva tecnología siempre tiene sus beneficios, pero muy pocos de sus usuarios se ha planteado lo que conlleva, en términos de seguridad el uso de máquinas virtuales; detalles de cómo se controla el tráfico entre máquinas virtuales dentro de una misma máquina real o cómo se gestiona el acceso a la red de éstas aunque tenga desplegada una solución de NAC (por no hablar de los problemas de seguridad en el hypervisor o el aislamiento eficaz entre máquinas virtuales) pueden presentar futuros quebraderos de cabeza a los responsables de seguridad de las organizaciones.

Sin llegar a ejemplos tan concretos como el de la seguridad en la virtualización, al final el objetivo principal es proteger la información como tal, sin descuidar su famosa triada sobre la que se sustentan la mayoría de capas de protección existentes: confidencialidad, integridad y disponibilidad, valores que seguramente en el pasado se controlaban dentro de una organización, pero que ahora son necesarios aplicar fuera de ella, puesto que la información referente a la misma se encuentra dispersa en multitud de fuentes. Qué se comenta sobre la organización o ciertos directivos en ciertos blogs, qué ficheros con información confidencial están en las redes P2P o quiénes están usando una marca o copyright sin autorización son, entre otras, preguntas que hay que formular para conocer de forma más global las amenazas. Éstas ya no sólo afectan a los activos de una organización, sino que afectan a activos más intangibles que muchas veces puede olvidarse de su existencia.

En definitiva, es imposible negar que los esfuerzos que se realizaban a finales de la década de los 90 en el área de la Seguridad de la Información no se parezcan mucho a los de hoy en día, ya que ni siquiera los esfuerzos realizados durante 2007 se parecerán a los de 2008. La sensación está en que en vez de cambiar unas actividades por otras, cada año se añaden nuevas capas pero no se quitan las anteriores, obteniendo como resultado la necesidad de un mayor presupuesto, recursos, procedimientos o formación. Igual que si fuera un efecto de 'bola de nieve', que rueda ladera abajo.

No todo está perdido, ya que al igual que las amenazas crecen y evolucionan, la capacitación y las herramientas que tenemos disponibles para hacer frente a estas amenazas, crecen y evolucionan. Tan sólo es necesario recabar todas las opiniones, dejarse aconsejar, y aunar esfuerzos para aproximarse cada vez más a un estado de seguridad controlada: evitando todos los riesgos que sea capaz, y protegiéndose contra los que asume. •

Para más información consulte en www.s21sec.com

"el objetivo que subyace en la mayoría de los ataques es siempre un motivo económico, pero muchas veces también ya se intercalan motivos políticos o relacionados con el espionaje industrial".

FOTO: www.sxc.hu / Craig Jewell

Un solo estándar ¿ES SUFICIENTE?

En una reciente reunión de bloggers, gente de Microsoft se dedicó a ensalzar las virtudes de OpenXML como nuevo formato de archivo y a compararlo con OpenDocument Format. La principal hipótesis de la reunión, que no se dilucidó, es si hace falta que un estándar sea único o si pueden coexistir dos o más. Y qué es más beneficioso. En esta nota vamos a ver si podemos dar una respuesta a esta pregunta.

Dos noticias se conocieron semanas atrás, que aparentemente no tienen relación entre sí. La primera, de mediados de febrero, indica que Toshiba anunció el cese definitivo de la producción y comercialización de los reproductores y discos del tipo HD DVD (1). El principal desencadenante fue la decisión de varios estudios de Hollywood de enfocarse en quien era el principal rival del HD-DVD: Blu Ray de Sony.

Un par de días después, Microsoft anunció que publicará documentación de sus APIs y otras especificaciones técnicas, incluyendo algunos de sus protocolos. Adicionalmente, pondrá a disposición de desarrolladores de open source algunas patentes (2). Lo que tienen en común ambas noticias es que se refieren a actividades dentro de una estrategia de definición de estándares. Dejando de lado las particularidades de cada una, lo cierto es que ambas son reacciones al reclamo de definición de estándares que está siendo cada vez más exigido (y exigente) en la industria. En rigor, somos víctimas de los estándares y, en más de una ocasión, de la multiplicidad de estándares. Aún hoy, quien viaje al exterior tiene que averiguar si en su lugar de destino hay 110 o 220 volts y cuántas patitas y de qué forma tienen sus enchufes.

La historia de los intentos de imponer estándares es harto conocida. El cassette de audio de Phillips triunfó ampliamente sobre el magazine de 8 pistas (cuyo verdadero nombre era 8-track cartridge) aún cuando éste precedió al cassette en dos o tres años. El compact disk tuvo un inmenso éxito popular por encima del DAT (Digital Audio Tape), del DCC (Digital Compact Cassette) y del minidisk, a pesar de lo cual estos tres formatos subsistieron en el ambiente del audio profesional.

También es muy conocida la historia del éxito del VHS de JVC sobre el Betamax de Sony y el Video 2000 de Grundig. En informática sabemos que si no hubiese sido por TCP/IP, POP3 y otros protocolos estándar, Internet no se hubiera masificado como lo hizo.

Sin embargo, el éxito o fracaso de un estándar no tuvo tanto que ver con su calidad tecnológica como con su inserción en el mercado y su capacidad de generar ganancias. A pesar de que IMAP (dicen los que saben) es más poderoso que POP, lo cierto es que POP sigue siendo, por lejos, el protocolo de correo electrónico más popular.

La respuesta a la pregunta del comienzo, si decir, si debemos tener uno o más estándares se contesta, en teoría, con la palabra "depende". O sea, depende del contexto, de la circunstancia, de la necesidad y, sobre todo, de la capacidad de solucionar un problema.

Para seguir con el ejemplo del copete, hay quienes sostienen que OpenDocument Format debería ser el próximo estándar en formato de documentos ya que posee las suficientes cualidades como para cubrir la mayor parte de las necesidades corporativas en un contexto de interoperabilidad y, sobre todo, del conocimiento abierto y extenso de la tecnología involucrada. Los defensores de OpenXML opinan que este formato hace exactamente lo mismo, con la ventaja de que permite conservar la compatibilidad retrógrada en las aplicaciones MS Office.

La pregunta es entonces, ¿cuál es el límite por el cual se debe elegir un estándar sobre otro? ¿Por qué hacen lo mismo en dos contextos distintos o por qué hacen cosas distintas en el mismo? ¿Cuántas features de diferencia hacen necesario cambiar un estándar por otro? ¿Seguiremos siendo, los usuarios, víctimas de la falta de acuerdo en los estándares?

En definitiva, y mientras no se determine, el criterio de selección debe ser siempre si este estándar resuelve mejor que el otro la problemática de mi cliente. Y no debería desviarme de ese objetivo.

La próxima pregunta es: ¿estándar de facto o estándar aprobado oficialmente? La veremos en otra oportunidad. ●

(1)http://www.vnunet.es/Actualidad/Noticias/Inform%C3%A1tica_profesional/Empresas/20080219009

(2)http://www.noticiasdot.com/wp2/2008/02/22/comunicado-oficial-de-microsoft-sobre-la-interoperabilidad-de-su-tecnologia/

Ricardo D. Goldberger
Periodista Científico especializado en Informática y Nuevas Tecnologías



El estándar de la IEEE 802.16 se ha convertido desde su aparición en 2001 en una tecnología que viene a solucionar los problemas de interconexión en zonas remotas y el alto costo de las redes cableadas. En este artículo veremos los principios de WiMAX y las generalidades de su funcionamiento.

Diego Javier Kreutzer
Jefe de Ing de Proyectos / TELMEX S.A.



FOTO: www.sxc.hu / Gabriella Fabbri

La aparición de WiFi generó una revolución entre las tecnologías inalámbricas ya que permitía conectarse a Internet desde casi cualquier parte. Los bares, restaurantes, shoppings y eventos de concurrencia masiva instalaron los primeros AP (access-point) que permitieron a los usuarios utilizar sus laptops y estar conectados fuera de sus hogares u oficinas.

Si para las redes WPAN (Wireless Personal Area Network), tecnologías como Bluetooth consiguieron eliminar los cables en los periféricos de una computadora, para redes WLAN (Wireless Local Area Network) WiFi (con bases en el estándar de la IEEE 802.11) se convertía en una excelente solución con gran ancho de banda; hoy en día los microchips de computadora en el mercado ya soportan esta tecnología.

Sin embargo, las distancias máximas logradas con WiFi eran de algunos metros, excelente para una red LAN pero no lo necesario para WMAN (Wireless Metropolitan Area Network). La necesidad de una red de banda ancha inalámbrica con un alcance muy superior a WiFi impulsó la aparición de un nuevo estándar que cumpliera estas expectativas, y allí es donde WiMAX aparece.

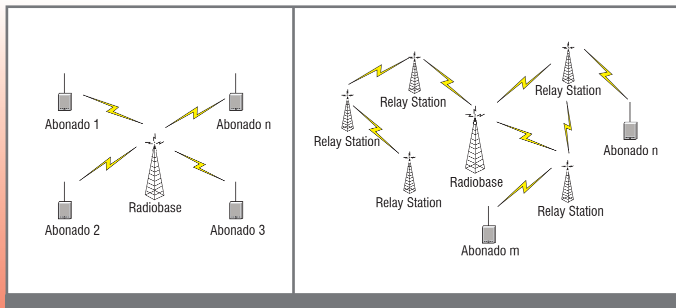


Fig. 1 - Redes

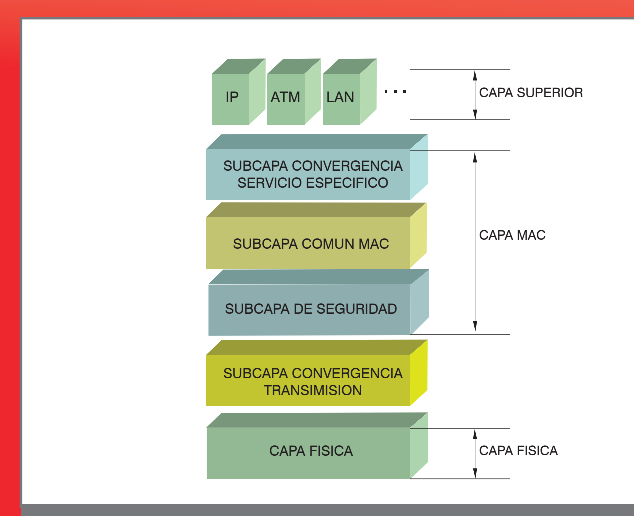


Fig. 2 - Modelo de capas



FOTO: www.sxc.hu / Jim Manning

¿Qué es WiMAX?

WiMAX significa Worldwide Interoperability for Microwave Access, o Interoperabilidad Mundial para Accesos de Microondas; es una tecnología inalámbrica de banda ancha que encuentra sus bases en el estándar de la IEEE 802.16 y es impulsada por el WiMAX Forum, un organismo sin fines de lucro cuya función es promover la interoperabilidad y compatibilidad de tecnologías wireless de banda ancha basados en dicho estándar. Con alcances de varios kilómetros y tasas de transmisión de 1 a 75 Mbps (según el estándar), la IEEE 802.16 aparece como una solución de última milla para redes WMAN de esta forma se convierte en una alternativa más económica a las redes cableadas (cable-modem, xDSL, fibra óptica) en términos de infraestructura y casi en la única opción para sectores geográficamente aislados, en donde tener cobertura con red cableada es inviable en términos de inversión para infraestructura. El primer estándar de la 802.16 fue difundido por la IEEE a fines del año 2001; operaba en la banda de frecuencias comprendida entre los 10 y 66 GHz y necesitaba indefectiblemente tener línea de vista (LOS) entre la radiobase y el equipo de abonado. El servicio que brindaba era únicamente para equipos fijos (no móviles). Posteriormente se publican los estándares 802.16a (banda de 2 a 11 GHz) y 802.16b/c/d (especificaciones de interoperabilidad), hasta que en junio de 2004 se publica la revisión de todas las versiones previas bajo la denominación IEEE 802.16-2004. Éste reemplaza a todos los anteriores e introduce algunas diferencias: sigue brindando servicios de acceso fijo, pero con importantes mejoras en el comportamiento frente a la interferencia multipath (recibir señal por múltiples caminos a causa de rebote en edificios) y a la robustez del sistema. Con la solución para los usuarios fijos en firme, el objetivo pasa a ser el mercado móvil; y la espera finaliza cuando en diciembre de 2005 la IEEE difunde la versión 802.16e para usuarios móviles.

Estructura de una red WiMAX

La tecnología WiMAX soporta dos modos de operación: el punto-multipunto (PMP) y el mallado (mesh). Una red con arquitectura PMP (ver figura 1.a) provee acceso de última milla para conectarse a Internet o a una VPN; la topología de la red para este caso consta de una radiobase BS (con acceso por ejemplo a Internet) y de equipos de abonado SS que tributan a la misma. El modo PMP requiere indefectiblemente línea de vista entre la BS y el SS. Una red con arquitectura de malla (ver figura 1.b), cuenta además con otro tipo de nodos denominados relay stations (RS); se trata de un tipo especial de SS que retransmite el tráfico de la BS a otro RS, o a un SS. Esta topología de red exige soporte a múltiples saltos para llegar de la BS a destino, pero permite expandir rápidamente la infraestructura con poca inversión de dinero frente a la infraestructura cableada. La radiobase está compuesta por la infraestructura de la misma (torre, energía, cableados, lugar físico, etc), el equipamiento WiMAX (arquitecturas variables de acuerdo a la necesidad puntual; WiMAX soporta el uso de antenas orientadoras y formadoras de haz, y sectorización para lograr mejor aprovechamiento del espectro y mejores distancias) y la conexión con el backhaul (vincula a la BS con el resto de la red y puede ser a través de líneas dedicadas, radios punto a punto, SDH, etc).

Modelo de capas

La arquitectura de capas de la IEEE 802.16 estándar se muestra en la figura 2, dividiéndose principalmente en dos capas principales: la capa física (PHY layer) y la capa MAC (Medium Access Control layer). La capa física en la banda de 10-66 Ghz (primer estándar IEEE 802.16) se basa en la modulación de portadora simple conocida como WirelessMAN-SC; dada la alta frecuencia de operación, requiere necesariamente línea de vista entre BS y SS. Con los sucesivos estándares, se proponen interfaces de aire para la banda de operación de 2 a 11 GHz, que ayudan a mitigar el efecto del multipath fading (mencionado anteriormente) y ofrecen flexibilidad en las soluciones WIMAX:

• **WirelessMAN-SCa**, utiliza un formato de modulación especial de portadora

única diseñado para NLOS.

- **WirelessMAN-OFDM**, utiliza multiplexación por división de frecuencia de vector ortogonal con 256 portadoras.
- **WirelessMAN-OFDMA**, utiliza acceso múltiple por división de frecuencia de vector ortogonal con 2048 portadoras.

En base a la relación señal-ruido del canal, se pueden seleccionar distintos esquemas de modulación: BPSK, QPSK, 16-QAM y 64-QAM, todos aplicables a la transmisión desde la radiobase al abonado (downlink) y desde el abonado a la radiobase (uplink). Una de las características más interesantes de WiMAX es proveer QoS (calidad de servicio), permitiendo tener tráfico de tiempo-real con necesidades más específicas de ancho de banda. Por tal motivo, la Capa MAC de WiMAX está orientada a la conexión e implementa mecanismos de control de planificación y admisión para los recursos de la red. En las especificaciones del estándar IEEE 802.16, se ofrecen dos modos de duplexión para manejar el tráfico uplink (de SS a BS) y downlink (de BS a SS): TDD (duplexión por división de tiempo) y FDD (duplexión por división de frecuencia). En el primer caso, sobre la misma frecuencia de portadora se divide la trama en intervalos de tiempo y se asigna uno de ellos para el tráfico uplink y otro para el downlink. En FDD, ambos tráficos se envían simultáneamente por dos frecuencias distintas, asignadas para tal fin. Esta posibilidad de manejar ambos esquemas de duplexión obedece a que WiMAX puede operar en bandas de frecuencia con y sin licencia, siendo en las licenciadas donde TDD se convierte en la opción más interesante.

Cada abonado negocia con la radiobase un perfil para transmitir sus datos basado en la QoS necesaria y en las condiciones del canal, siendo la radiobase quien determine cuál será el resultado de esa negociación. En la figura 3 puede verse la estructura de trama (frame) que se transmite entre BS y SS. En TDD cada frame MAC incluye un subframe downlink seguido por un subframe uplink; en el caso de FDD, el subframe uplink podría enviarse retrasado con respecto al downlink para que los SSs puedan recibir la información necesaria acerca del canal de acceso. En una arquitectura PMP, todas las transmisiones entre la BS y los SSs son coordinadas por la BS. El subframe downlink utiliza TDM, de tal manera que la BS asigna cada intervalo de tiempo para cada SS registrado; mientras que el subframe uplink utiliza TDMA, es decir son solicitudes por demanda. En el subframe downlink, se transmiten los mensajes downlink MAP (DL-MAP) y el uplink MAP (UL-MAP), que comprenden las asignaciones de ancho de banda para transmitir datos en ambas direcciones. De hecho, las longitudes de los subframes uplink y downlink son determinados en forma dinámica por la BS y son difundidos a las SSs a través de los mensajes UL-MAP y DL-MAP en el comienzo de cada frame. Esta funcionalidad contempla que la mayoría de las aplicaciones de Internet tienen mayor tráfico downstream que upstream (ancho de banda asimétrico), pudiendo ajustar el ancho de banda asignado en cada dirección en forma dinámica. La asignación de recursos en una arquitectura PMP es crítica; se tienen múltiples SSs compartiendo un mismo tráfico uplink al BS en base a la demanda de cada uno. Si un SS necesita determinado ancho de banda, hace una reserva a la BS enviando un requerimiento; en aceptación al mismo, la BS debe determinar y asegurarle la posibilidad de transmisión en los time-slots del frame usando algún algoritmo de planificación aplicable a todas las SS autorizadas. En WIMAX, se sugieren dos métodos para tal fin: centralized polling o contention-based random access, es decir, consulta o contienda. En el primer caso, cada SS está autorizada a enviar su requerimiento sólo cuando es consultada por la BS; en el segundo caso, todos los SS compiten por obtener una oportunidad de transmitir sus requerimientos utilizando mecanismos de contienda. En redes poco saturadas, el acceso random (contienda) parece ser el mejor camino; pero a medida que crece la carga sobre la red, prevalece el método de consulta. La interfase entre la capa PHY y la capa MAC se trata como una subcapa separada, denominada subcapa de convergencia de transmisión y su función es ocultar los detalles de las especificaciones en la capa PHY de la capa MAC. Esta subcapa transforma MPDUs (unidades de la capa MAC, se verán a continuación) en bloques de longitud fija denominados TC PDU (Transmision Convergence Su-

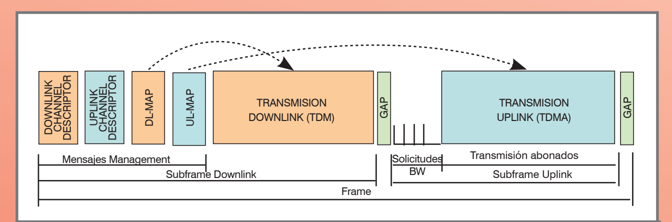


Fig. 3 - Estructura de trama TDD en arquitectura PMP

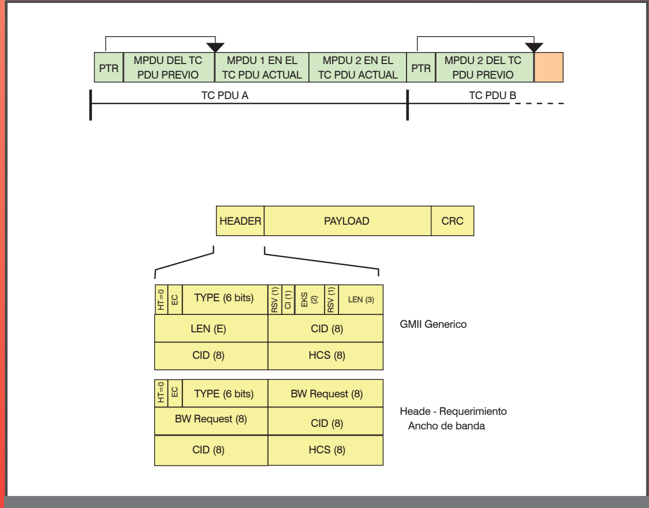


Fig. 4 - Formato

WiMAX en la última milla

Una forma en el que los WSP integran WiMAX como última milla es manejando el tráfico en Ethernet desde el usuario hasta su red. El equipo de abonado (de fácil instalación en terrazas o en mástil) provee acceso a la red del proveedor a través de una interfase 10/100 BT; de esta forma, se puede conectar directamente una placa de red Ethernet de cualquier dispositivo que maneje dicho protocolo. Del lado del nodo de WiMAX, también se baja en Ethernet hasta el switch o router de servicio pudiendo configurarse como troncal (IEEE 802.1Q); permitiendo la implementación de VLANs se puede separar el tráfico de los distintos abonados, y armar una VPN distinta para cada uno.

blayer Protocol Data Units); estos comienzan con un puntero que indica dónde inicia el encabezado del próximo MAC PDU en el bloque. El formato del TC PDU (ver figura 4.a) permite resincronizar un MAC PDU si el bloque anterior sufrió errores irrecuperables. Pasando ahora a la capa MAC, en la misma se encuentran 3 subcapas:

• **Subcapa de seguridad**: Su función es proveer control de acceso y confidencialidad en el enlace de datos. Para tal fin, esta subcapa cuenta con un protocolo de encriptación para el tráfico a través de la red, y un protocolo de privacidad y manejo de claves (PKM), para asegurar una distribución segura de claves entre BS y SS, con fines de autenticación. Wimax soporta AES (Advanced Encryption Standard) y 3DES (Triple Data Encryption Standard). Según IEEE 802.16-2001, transmitir el header y el mensaje de management sin encriptación facilita el registro de los usuarios y la operación normal de la subcapa MAC; pero también facilita la introducción de mensajes falsos. En el último estándar 802.16e, a fin de garantizar mayor seguridad el payload del MPDU se encripta con DES en el modo CBC o AES en el modo CCM.

• **Subcapa Común MAC**: Es el núcleo de la capa MAC 802.16. Define todos los métodos de control de conexión, distribución de ancho de banda, procedimientos de acceso al sistema y solicitud automática de repetición. Cualquiera sea el servicio solicitado –y aunque éste no involucre una necesidad de conexión por su naturaleza de tráfico- debe establecerse una conexión con la radiobase que provea un mecanismo para que el SS haga la solicitud del ancho de banda necesario en base al servicio a transmitir (QoS) y provea información de transporte y de control; de esta forma, la radiobase asigna un identificador de conexión (CID) a cada una de ellas para poder planificar el manejo de los recursos de la red. El CID está compuesto por 16 bits y se obtiene en el momento en el que la SS se une a la red. Cada SS tiene una dirección MAC estándar (48 bits) que identifica unívocamente al equipo; al entrar en la red se asignan 3 conexiones de management: la conexión básica (control de enlace de radio, etc), la conexión primaria (autenticación y establecimiento de la conexión con BS) y la conexión secundaria (transferencia de mensajes de management, como DHCP, TFTP, SNMP). Además de estos mensajes de management, los SSs se asignan conexiones de transporte unidireccionales (se asignan de a pares, uplink y downlink). El MPDU (MAC Protocol Data Unit) es el frame que intercambian la BS y el SS y consiste de 3 partes: un encabezado de longitud fija (contiene información de control); un payload de longitud variable y un chequeo de error (FCS). Los MPDUs pueden tener dos tipos de encabezado (ver figura 4.b): el genérico (GMH o Generic MAC Header) y el de requerimiento de ancho de banda (BRH o Bandwith Request Header). Dentro del primer tipo, puede tratase de un MPDU llevando uno o varios MSDU (donde el payload es información de las capas superiores obtenida a través de la capa de convergencia) o de un MPDU llevando información de management. El segundo tipo se envía sin payload y tiene el bit HT (Header Type) en "1".

• **Subcapa de convergencia de servicio específico**: brinda soporte para varios tipos de protocolos, como IP, ATM, Ethernet, Virtual LAN y PPP (hoy en día orientada a IP y a Ethernet). Encapsula los frames provenientes de las capas superiores MSDUs (MAC Service Data Units) en MPDUs (MAC Protocol Data Units) y viceversa.

Alcances de la red WiMAX

El desarrollo de WiMAX fue enfocado a las necesidades de QoS, alta seguridad, flexibilidad, interoperabilidad, movilidad, bajo costo y alta capacidad. Características como estas fueron puntos claves para que se la viera como una opción de backhaul de larga distancia. Hasta ahora, el backhaul montado en tecnologías wireless contemplaba circuitos E1 o T1, sobre redes SDH y SONET. Sin embargo, la utilización de Ethernet como protocolo dominante en la infraestructura de hoy y el avance de las redes Metro-Ethernet y de SDH de nueva generación (SDH NG) hacen que WiMAX sea fácilmente integrable como backhaul de red vinculados por Ethernet.

La incorporación de fabricantes de microprocesadores al WiMAX Forum indica que en el corto plazo WiMAX estará embebido en las computadoras y demás dispositivos personales; y ciudades como Seul ya implementaron WiMAX, brindando servicio tanto a estaciones fijas como a usuarios móviles. En adelante, el desafío será integrar las especificaciones de la IEEE 802.16-2004 con la IEEE 802.16e ya que la primera fue ideada para usuarios fijos y la segunda para usuarios móviles, a fin de poder reunirlas en un mismo estándar que contemple todas sus virtudes. ●

Acerca del autor

Diego Javier Kreutzer es Ingeniero en Electrónica egresado en 1999 de la Universidad Nacional de La Matanza. Actualmente se desempeña como Jefe de Ingeniería de Proyectos en TELMEX S.A. Anteriormente trabajó en Telefónica de Argentina y en Impsat S.A.

Convivencia entre WiFi y WiMAX

La principal limitación de WiFi es proveer acceso solamente a nivel LAN (el Access-point soporta pocos metros, y es necesaria una última milla contra el Wireless Service Provider) pero está altamente difundido y los dispositivos ya vienen preparadas para dicho estándar. Por el contrario, WiMAX fue diseñado como última milla con requerimientos particulares (QoS) a bajo costo; pero no está lo suficientemente integrado en dispositivos móviles, PDAs y otros equipos. En base a esto, WiMAX es la opción que provee la última milla para interconectar los AP de WiFi con los Carriers en un ambiente wireless.

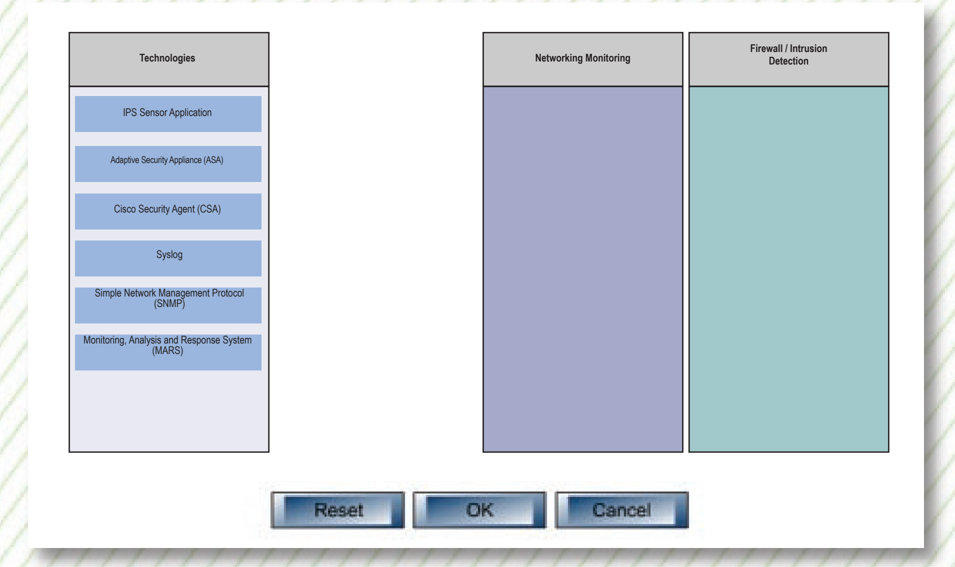
Hasta tanto WiFi no consiga expandir su cobertura lo necesario para prescindir de la última milla y el soporte para WiMAX no esté integrado a los microprocesadores logrando tamaño pequeño y bajo costo, la convivencia entre ambas continuará por algún tiempo más.

Certificaciones

Ponga a prueba su conocimiento con las preguntas del exámen 640-802 de certificación CCNA de Cisco.



Una la tecnologia de la izquierda con su correspondiente categoria de la derecha



Para más información visite:

www.transcender.com - www.transcender.com/demos

Respuesta correcta



Explicación

Syslog, Simple Network Management Protocol (SNMP), y Monitoring, Analysis, y Response System (MARS) son aspectos de monitoreos de la red. El IPS Sensor Application, Adaptive Security Appliances (ASAs), y Cisco Security Agent (CSA) son partes del firewall o del sistema de intrusion detection.

Estos son los componentes del firewall y del módulo de intrusion detection en la tecnología Threat Detection and Mitigation de Cisco:

- IPS Sensor Application
- Adaptive Security Appliance (ASA)
- Cisco Security Agent (CSA): Usado para la protección endpoint durante el proceso de detección de amenazas y mitigación.
- PIX: Es un firewall appliance utilizado para filtrar el tráfico de red y bloquear el tráfico no deseado.
- FWSM: Catalyst 6500 Firewall Services Module.
- IOS firewall: Característica del Cisco Internetwork Operating System.
- Intrusion Prevention System (IPS): Característica del Cisco IOS.

Estos son los componentes del modelo de monitoreo de la red en la tecnología Threat Detection and Mitigation de Cisco:

- Syslog: Mantiene la información de log y es una característica del Cisco IOS.
- Simple Network Management Protocol (SNMP): Característica del Cisco IOS utilizada para la administración de red.
- Monitoring, Analysis, and Response System (MARS): Brinda un monitoreo seguro de las redes host y las aplicaciones.
- NetFlow: Característica de Cisco IOS.
- Cisco Traffic Anomaly Detector Module: Utilizado para detectar ataques denial-of-service (DoS).

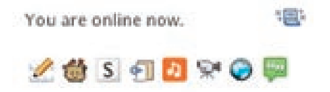
facebook Profile edit Friends Networks Inbox home account privacy logout

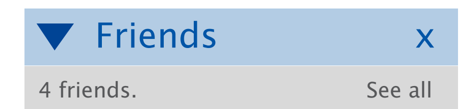
Mark Zuckerberg

El niño mimado de la Web

Hace cuatro años Mark Zuckerberg no tenía ni auto, ni casa, ni trabajo. Hoy, con tan solo 23 años y el look descontracturado de un universitario, es el CEO de una de las comunidades sociales más grande de la Web, Facebook. ¿Cómo lo hizo? "Hackeando", responde.

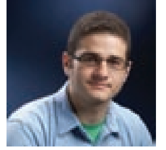
View photos of you (3)
View videos of you (1)
Edit my profile





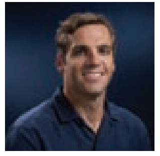
Friends X

4 friends. See all



Dustin Moskovitz

Adam D'Angelo



Owen Van Natta



Chamath Palihapitiya



Mini-feed





"Realmente todo pasó de una forma muy interesante", cuenta Zuckerberg, quien vive en un departamento alquilado y tiene solo una mesa y dos sillas como muebles. Pero esta imagen no suena ilógica si pensamos que hablamos de un joven de 23 años. Pero cuando aclaramos que hablamos del CEO y fundador de la sexta página más visitada a nivel mundial y que ostenta más de 65 millones de usuarios activos, las cuentas no cierran.

Ya de chico en los suburbios de Nueva York, donde nació y fue criado, Mark vio crecer su interés por las computadoras, tanto que ya en la secundaria junto a un compañero diseñaron un plug-in para el reproductor de MP3 Winamp el cual era capaz de aprender de los gustos musicales y crear una lista de reproducción con ese patrón. Gracias a este desarrollo obtuvieron sus primeras ofertas de trabajo por parte de Microsoft y AOL. La respuesta fue un no rotundo para iniciarse en el mundo universitario y estudiar de Ciencias de la Computación en Harvard. Donde todo comenzó.

Para entonces, en 2003, la universidad no tenía una versión online del llamado "face book", libro al cual recurren los alumnos para conocer información básica y fotos de los demás compañeros. "Me decían constantemente que no se podía tener esta información, yo solo les quise demostrar que sí era posible", explica Zuckerberg. Para esto irrumpió una noche en los archivos de los alumnos y creó un sitio llamado Facemash, el cual mostraba aleatoriamente fotos de los estudiantes para conocer al más popular. Luego de cuatro horas, 450 visitas y 22 mil fotos vistas,



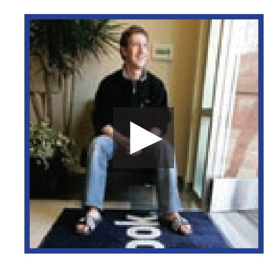
Harvard le quitó la conexión a Internet a Zuckerberg. ¿La razón? Infringir la seguridad informática y violar las políticas de privacidad y de propiedad intelectual.

Luego de las disculpas correspondientes, en febrero de 2004 junto a Dustin Moskovitz and Chris Hughes decidieron poner online a Thefacebook.com, como se lo llamó originalmente, para toda la comunidad de la Universidad. Con solo dos semanas de existencia, más de la mitad del alumnado se había inscripto. Ya para marzo decidieron ampliarse e incluir otras universidades como Standford, Columbia y Yale y más de 30 colleges.

En septiembre de 2006 se abre Facebook.com al mundo: cualquiera con una dirección válida de e-mail podía formar parte de esta red social y de esta forma logran llegar a los 12 millones de usuarios activos al término del año.

Pero, ¿cómo se mantiene facebook.com? Principalmente gracias a la publicidad y a los sponsors. Por ejemplo Apple fue una de las primeras empresas en demostrar su apoyo esponsoreando un sitio para los entusiastas del iTunes. Sin embargo, el apoyo económico más fuerte viene de otro lado, de un acuerdo con Microsoft en el cual el gigante de Redmond puede poner banners publicitarios en el sitio hasta 2011.



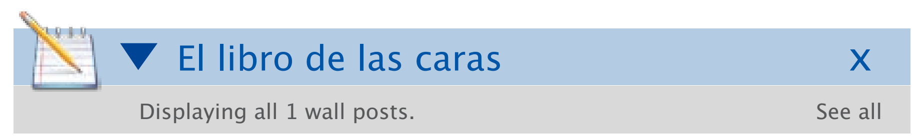


www.NexMedia.com.ar

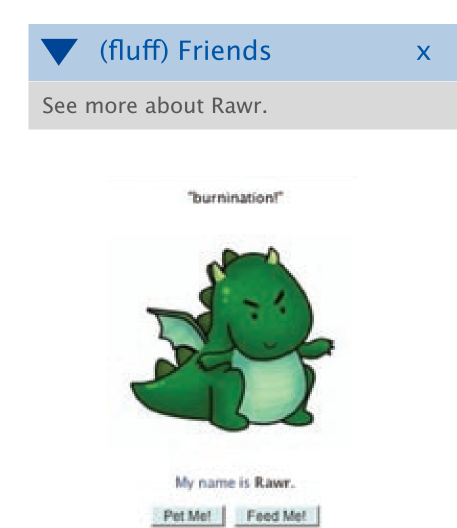


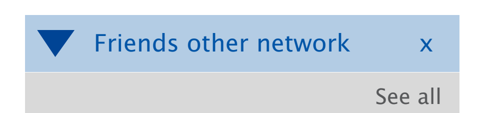
Para saber un poco más de la historia de Mark Zuckerberg y de cómo surgió una de las redes sociales más importantes de la Web, no se pierda el video en la web de NexMedia.

Saber de tecnología es saber de negocios.



Facebook es un sitio social que ayuda a la comunicación entre las personas, entre amigos, familia y compañeros de trabajo y mediante el cual se puede compartir información, eventos, fotografías, gustos y grupos. Con solo una dirección válida de Internet uno se puede loggear y formar parte de esta comunidad social. Uno puede compartir con sus amigos fotografías, música, enviar y recibir mensajes y conectarse con gente de todo el mundo. Facebook representa el segundo sitio PHP más visitado del mundo y tiene una de las bases de datos MySQL más grande con cientos de bases de datos corriendo al mismo tiempo. Además, tiene un ligero pero potente marco multi-idioma RPC que permite vincular los subsistemas escritos en cualquier idioma y correrlos en cualquier plataforma. Una de las características de Facebook es que es una plataforma que permite que desarrolladores e ingenieros construyan nuevas y propias aplicaciones y herramientas y las pongan a disposición de la gran cantidad de usuarios de esta red social. Hasta el momento se han registrado más de 10 mil herramientas las cuales permiten compartir música y gustos hasta prestar dinero o compartir archivos. Para más información acerca de la Plataforma Facebook visite http://developers.facebook.com/





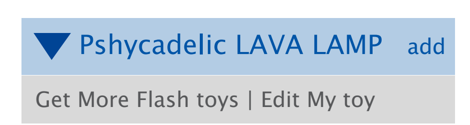
Networks with the most friends
Argentina (4)

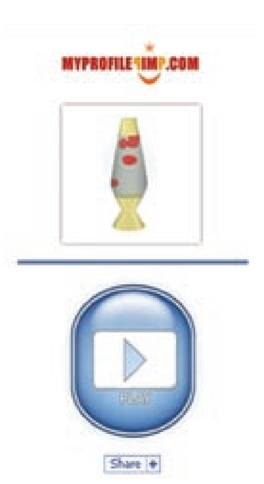
Networks you belong to
Italia (7)

Networks you belong to
Francia (4)

Networks you belong to
Canada (2)

Show All Networks | View All Friends





 Línea del tiempo de facebook x



2004

- **Febrero:** Mark Zuckerberg y sus co-fundadores Dustin Moskovitz y Chris Hughes inician Facebook desde su cuarto de Harvard.
- **Marzo**: Facebook se expande de Harvard a Stanford, Columbia y Yale.
- **Junio**: Facebook muda su centro de operaciones a Palo Alto, California.
- **Septiembre:** Se agrega la aplicación de grupos y The Wall pasa a formar parte del Profile.
- **Diciembre:** Llega al millón de usuarios activos.



2005

- **Mayo:** Facebook alcanza las 800 redes.
- **Agosto:** La compañía cambia oficialmente su nombre de thefacebook.com a Facebook.
- **Septiembre:** Facebook se expande para agregar las escuelas secundarias nacionales e internacionales.
- **Octubre:** Se agrega la aplicación de las fotos.
- **Diciembre:** Facebook llega a más de 5.5 millones de usuarios activos.



2006



- **Mayo:** Se agregan las redes laborales.
- **Agosto:** Se agrega la plataforma de desarrollo. Se agrega la aplicación de Notas. Facebook y Microsoft cierran el acuerdo de publicidad.
- **Septiembre:** Se introducen las aplicaciones News Feeds y Mini-Feed con control de privacidad. Facebook se abre al mundo para que cualquier usuario se pueda registrar.
- **Diciembre:** Facebook llega a los 12 millones de usuarios activos.



2007

- **Febrero:** Se agrega como característica la Virtual Gift Shop.
- **Marzo:** Facebook llega a los 2 millones de usuarios activos en Canadá y al millón en Gran Bretaña.
- **Abril:** Facebook llega a los 20 millones de usuarios en todo el mundo. Se actualiza el diseño del sitio y se agregan nuevas redes.
- **Mayo:** Se agrega la aplicación Marketplace. Facebook alcanza los 65 desarrolladores con más de 85 aplicaciones.
- **Julio:** Facebook compra Parakey.
- **Octubre:** Se llegan a los 50 millones de usuarios. Facebook y Microsoft expande el acuerdo para abarcar el mercado internacional.

La psicología de

Los usuarios de las computadoras estamos, hoy en día, inundados con gran cantidad de información, y el tomar conciencia de esta cantidad de material puede volverse una tarea bastante dificultosa. De lograr que esta dificultad aminore mediante el estudio y el diseño de tecnología de avanzada y de la interacción de técnicas que mejoren las capacidades humanas es de lo que se encarga el grupo de investigación de visualización e Interacción de Microsoft Research, liderado por Mary Czerwinski.

Para ello exploran técnicas perimetrales de concientización para preservar la cantidad de tareas de los usuarios y minimizar las interrupciones. ¿Por qué? Desde el grupo Visualization and Interaction for Business and Entertainment afirman que es bastante difícil recordar qué es lo que uno estaba haciendo antes de una interrupción, al igual que recuperar el contexto de trabajo en el que se estaba. Para esto, su foco de trabajo se centra en el desarrollo de nuevas formas de visualizar el flujo de las tareas. "Generalmente en Windows, las notificaciones surgen en lugares en donde uno no está prestando atención, surgen ventanas en los lugares menos esperados o su tamaño no tiene relación con su contenido. Es por esto que buscamos la creación de nuevas soluciones para lograr que el contenido importante esté más al alcance del usuario y de forma tal que sea de fácil interacción en cualquier dispositivo", explica Czerwinski.

Por un lugar se empieza

En 2003, momento en el que comenzó el grupo, el foco principal de investigación era buscar nueva tecnología que permitiera realizar varias tareas al mismo tiempo y encontrar la forma en la que el software debía estar diseñado para afrontar la nueva forma de trabajo que estaba adquiriendo la gente.

Para resolver esta problemática se creó un logger, llamado VIBE logger, el cual registra la forma en que la gente usa las ventanas al trabajar con ellas hoy en día. El estudio incluía un completo y exhaustivo informe en el que se detallaban todos los movimientos del usuario referidos a la utilización de las ventanas, su tamaño, configuración, etc. Por ejemplo, uno de los resultados fue darse cuenta que el usuario tiende a deja cada vez más las ventanas abiertas y monitorear el trabajo desde allí y de esta forma, también, tener un navegador Web, un documento de Word y uno de Excel abiertos al mismo tiempo ya que se debe trabajar con los tres juntos. ¿La solución? Herramientas que permitieran mantener varios documentos relacionados abiertos al mismo tiempo en la periferia.

Es decir, gracias a ese estudio se pudo tener por primera vez en Microsoft un documento que detallara las claves a tener en cuenta para luego poder diseñar una mejor interface y de esta forma lograr una mejor interacción.

Carrera de Psicología en Microsoft

Si bien el área de estudio de Czerwinski estuvo enfocado en entender la psiquis humana y la llevó a estudiar Psicología en la universidad Ball State, "siempre estuve interesada en la ciencia y mi pasión por la investigación de la psiquis y los procesos de información visual me llevaron eventualmente a tener un PhD en psicología cognitiva", confiesa.

Como parte de ese PhD, desarrollado en la universidad de Indiana, se fue inmiscuyendo en el mundo de las computadoras, a la experiencia de la programación, el análisis, etc. "Me entusiasme mucho con esta nueva área de investigación, en donde los problemas psicológicos se mezclaban con las metáforas computacionales y los modelos, es decir el campo de la interacción computadora-hombre (HCI), hasta que comencé a trabajar en Bellcore y me di cuenta que realmente no sabía nada sobre HCI. Mis primeros tres meses fueron en la biblioteca del campus leyendo libros sobre este tema", explica.

Gracias al conocimiento que le brindó la psicología, su objetividad a la hora de

la computación

utilizar la información del usuario y no su propia intuición, las habilidades de buena comunicación y una fuerte responsabilidad fue el conjunto de capacidades que le abrió la puerta de diversas experiencias laborales: de Bellcore a la NASA-Johnson Space Center, Compaq Computer Corporation para arribar, finalmente a Microsoft.

Luego de dos años de estar a cargo de un grupo de ingenieros en el Interactive Media Group de Microsoft, en 1997 se unió al grupo User Interface Research (el que actualmente se llama Adaptive Systems and Interaction) en Microsoft Research para enfocarse de lleno al campo de la investigación.

En la actualidad es investigadora del Human-Centered Computing (HCC) y es la encargada del grupo de investigación Visualization and Interaction (VIBE).

Les contamos cuáles son algunos de los últimos proyectos desarrollados por el grupo de investigación:

• **StepUI:** una aplicación que puede ser controlada mediante pasos de baile en vez del cursor del mousse. Con StepMail se pueden leer, borrar o marcar los e-mails y con StepPhoto organizar todas sus fotografías. De esta forma se utiliza un dispositivo que es divertido de usar y que lo mantiene de pie y activo y por sobre todo lejos de la silla.

• **GroupBar:** Es una liviana herramienta de escritorio que permite una administración más efectiva de las ventanas en la barra de tareas. Puede arrastrarlas, reubicarlas, agruparlas y elegir la opción de ver múltiples ventanas al mismo tiempo.

• **StatusWriter:** utiliza el sistema VibeLog para grabar toda la actividad de un usuario en la PC. El proyecto aún está en su face inicial.

• **MPTrain**: es un dispositivo que monitorea los latidos de su corazón y la velocidad en la que corre y de acuerdo a los datos obtenidos reproduce la música correcta para de esta forma estimularlo y alcanzar así mejores resultados. ●

Más Información

Mary Czerwinski

http://research.microsoft.com/~marycz/

VIBE: http://research.microsoft.com/research/vibe/

"Me entusiasme mucho con el área de investigación en donde los problemas psicológicos se mezclaban con las metáforas computacionales y los modelos, es decir el campo de la interacción computadora-hombre (HCI), hasta que comencé a trabajar en Bellcore y me di cuenta que realmente no sabía nada sobre HCI. Mis primeros tres meses fueron en la biblioteca del campus leyendo libros sobre este tema".

Mary Czerwinski



LA POTENCIA DE LA VIRTUALIZACION

IBM expande su cartera de hardware y software para ayudar a las empresas a virtualizar los recursos tecnológicos permitiéndoles ahorrar dinero, energía y espacio.

IBM anunció que está haciendo llegar su tecnología basada en microprocesadores POWER6 a pequeños y medianos clientes y entregando nuevas ofertas de virtualización diseñadas para ayudar a esos clientes a consolidar la capacidad de sus servidores, ahorrar energía y administrar de una manera más eficiente sus costos de tecnología informática.

La virtualización permite a las empresas reducir el consumo de energía hasta en un 80 por ciento, administrar mejor el crecimiento de sistemas y lograr reducciones en el costo total de propiedad de hasta 72 por ciento. Además, hace posible que múltiples funciones de servidor se ejecuten en una menor cantidad de servidores.

Abordando estos requisitos, IBM introdujo una nueva plataforma de virtualización – Power VM Express- especialmente diseñada para permitir a los clientes PyME administrar mejor sus costos de tecnología informática, impulsar la máxima eficiencia en el consumo de energía y aumentar la utilización de recursos. PowerVM proporciona soluciones de virtualización que incluyen AIX - el sistema operativo UNIX de IBM, Linux, e i5/OS para clientes de System i. En combinación con los nuevos servidores System p basados en el microprocesador POWER6 y servidores BladeCenter los clientes pueden crear hasta 160 particiones virtuales en un único sistema, mejorando el aprovechamiento de los servidores.
"La virtualización en general ha estado dentro del dominio de las grandes empresas. Hoy apuntamos a simplificar la adopción de tecnologías de virtualización, al ponerlas a disposición de las pequeñas y medianas empresas," comentó Scott Handy, vicepresidente de marketing y estrategia para IBM Power Systems. "Las capacidades que brindamos cuando combinamos el software de virtualización líder de IBM y la tecnología POWER6 en nuestras ofertas nos llevan más allá del rendimiento de primer nivel mundial y nos permiten ayudar a los clientes a construir empresas más eficientes mediante el ahorro de tiempo, espacio y dinero."

El software PowerVM – antes conocido como POWER Virtualization (APV) – ahora está disponible en las versiones Express, Standard y Enterprise. Una característica es que permite a los servidores System p ejecutar aplicaciones binarias Linux x86 no modificadas sin recompilación, además de aplicaciones UNIX y Linux sobre POWER. Según IDC, se estima que el gasto en software y servicios de virtualización superará los USD 15 mil millones en todo el mundo hacia 2011, en comparación con USD 6.500 millones en 2006.

Muchos de los atributos de la tecnología de virtualización ahora están siendo utilizados por clientes grandes y pequeños. Casi 70 por ciento de servidores System p basados en procesadores IBM POWER6 utilizan la tecnología PowerVM hoy día. Además de la gestión de sistemas y los beneficios de costos, la plataforma PowerVM proporciona a los clientes nuevas opciones para mejorar la disponibilidad de sistemas y aplicaciones, permitiendo reducciones o la eliminación de las paradas planificadas. •

FOTO: www.sxc.hu / Alessandro Paiva

Beneficios de PowerVM

- Lo ayuda a reducir el costo de la infraestructura en un 62 por ciento.
- Aumenta la flexibilidad de su negocio permitiéndole anticiparse a las necesidades y requerimientos.
- Reduce la complejidad de su gran infraestructura.

Componentes de PowerVM

PowerVM está disponible es todos los servidores Power Systems incluyendo en BladeCenter JS21 y JS22 y la combinación de un mayor control del hardware y software. PowerVM incluye:

- **Live Partition Mobility:** Diseñado para permitirle mover una partición desde un servidor físico a otro servidor compartido sin la interrupción de las aplicaciones.
- **Virtual I/O Server:** Es una partición especial la cual brinda recursos virtuales de I/O a las particiones clientes. El Virtual I/O Server está diseñado para reducir costos mediante la eliminación de la necesidad de adaptadores dedicados de redes, adaptadores de discos y drivers.
- **Integrated Virtualization Manager:** Permite chequear, clickear y consolidar la carga de trabajo a través de su interfaz. Con IVM se puede particionar un sistema, incluyendo la creación de LPARs, y la administración del almacenamiento virtual y Ethernet virtual.
- **Micro-Partitioning y procesadores compartidos LPARs:** Con la utilización de Micro- Partitioning en un servidor Power System puede crear múltiples particiones virtuales con un procesador. Esto permite capitalizar los recursos que ya se tienen y aumentar la utlización del servidor sin sacrificar la disponibilidad y disminuyendo el costo total.
- **Shared Dedicated Capacity:** Mediante esta característica se logra una optimización del sistema sin comprometer el poder de cómputo de los trabajos críticos en procesadores dedicados.



CASO DE EXITO

OSRAM SYLVANIA, líder en soluciones de iluminación y productos especializados con diseño innovador y tecnología de ahorro de energía, estaba a punto de llegar al máximo de la capacidad de servidores y quería evitar actualizaciones costosas a sus sistemas existentes. La compañía enfrentaba el desafío de reducir significativamente sus costos operativos mientras se enfocaba en la implementación de una nueva estrategia a cinco años. Los servidores IBM System p, la tecnología de virtualización PowerVM y los servicios de migración de IBM proporcionaron la solución correcta.

"Cuando investigamos el problema, nos convencimos de que IBM ofrecía el mejor soporte para la transición, la mejor tecnología para operaciones y la mejor estrategia para el desarrollo de largo plazo," señaló Jeffrey Ruck, director de servicios de infraestructura tecnológica de OSRAM SYLVANIA. "En dos proyectos por separado, pudimos consolidar un total de 61 servidores UNIX y x86 de HP y Dell a 11 servidores System p que ejecutan AIX. Los equipos de Fábrica de Migración y Consolidación de Servidores x86 de IBM lideraron el proyecto, y como resultado, la respuesta del sistema es el doble de rápida, el espacio de CPU se ha reducido cuatro veces, y pudimos entregar mejores resultados de negocios con menos consumo de energía y menos refrigeración, y con costos de licencia significativamente más bajos".

FOTO: www.sxc.hu / Quentin Houyoux

HYPER -V

Se trata de Windows Server 2008 RC1 Enterprise con la versión beta de Hyper-V para evaluar la nueva tecnología, probar las aplicaciones y planear sus proyectos de consolidación, continuidad empresarial y alta disponibilidad. La versión beta estaba programada para entregarse en el primer trimestre del 2008 con la versión para fabricación (RTM) de Windows Server 2008.

Hyper-V, formalmente conocido como "Veridian", difiere bastante de los productos de virtualización de Microsoft marcados como Microsoft Virtual Server, y utiliza un hypervisor para la abstracción de los servicios de hardware al entorno del OS y para la localización y partición de recursos. Esto se diferencia de productos como Microsoft Virtual Server, VMWare Server y VMWare Workstation, Parallels, Linux KVM y Virtualbox, recientemente comprada por Sun, la cual utiliza una técnica conocida como virtualización host-based en la cual un sistema operativo nativo como Windows o Linux corre un subproceso de su kernel nativo llamado Virtual Machine Monitor (VMM) para brindar servicios virtualizados a una máquina virtual, como ser CPU virtual, memoria y dispositivos. Un hypervisor, por otro lado, es una fina capa abstracta la cual bootea sobre el hardware nativo que realiza algunas funciones del kernel del sistema operativo, pero abstrae mucho de lo necesario para correr un sistema operativo múltiple con sus aplicaciones por sobre todas. La ventaja de la virtualización basada en un hypervisor es que tiende a ser más rápida y escalable. La desventaja, por otro lado, es que el hypervisor tiende a ser realmente muy dependiente del hardware y usualmente necesita de una aceleración, como las extensiones "VT" de Intel o "Pacifica" de AMD presentadas en los chips Xeon u Opteron, como las soluciones basadas en Xen y Hyper-V, y requiere de modificaciones del kernel del sistema operativo y de un dispositivo especial de paravirtualización para ser corrido en el entorno VM para facilitar la performance de la red.
ESX de VMWare difiere de Hyper-V y Xen en que utiliza virtualización basada en software, por lo que no necesita las extensiones de VT o Pacífica. P, posee un entorno más restringido en cuanto en qué tipo de hardware puede correr. ESX Server también necesita de un file system especial conocido como VMFS para guardar las imágenes de la máquina virtual para lo que se debe dedicarle una SAN-based LUN. Por el otro lado, Hyper-V puede correr en cualquier sistema moderno que soporte Windows 2008 de 64-bit, almacena todas sus máquinas virtuales en un di-



El esperado Windows Server 2008 está ofreciendo sus mejores adelantos. Clientes y socios disponen de una versión beta de su tecnología de virtualización de servidor basada en el hypervisor, denominada Hyper-V.



rectorio regular en NTFS, y provee soporte de drivers third-party y built-in mediante el uso del llamado sistema operativo "Parent" como mecanismo pass-thru. En lenguaje Xen, esto también está referido como "Domain 0", en donde el soporte de dispositivos y del file system es provisto por el kernel de Linux (o en el caso de Sun xVM, Solaris) y file system de Linux como ext3 y ReiserFS.

Instalación, uso y performance

No es ninguna sorpresa que la arquitectura de Hyper-V es muy similar a la de Xen, luego de que en 2006 Microsoft y XenSource -ahora parte de Citrix Systems- realizaran una alianza para compartir tecnología. Lo único que se debe hacer para utilizar Hyper-V es realizar una instalación por default del Windows Server 2008, lo que tomará 20 minutos en una máquina Opteron dual-core, luego ir al Windows 2008 Server Manager y elegir la opción "Add New Role" y seleccionar el servidor "Hyper-V".

Luego de unos minutos de configuración y reinicio, Hyper-V inicia Server 2008 y se podrá comenzar con una nueva Máquina Virtual usando las herramientas del Hyper-V Microsoft Management Console (MMC). Luego de instalar la máquina virtual, lo que puede realizarse vía CD-ROM/DVD media o mediante un archivo ISO, se deberá instalar el Integration Components (similar a las VMWare Tools) para mejorar la performance en red y el soporte del hardware paravirtualizado. Para sistemas operativos guest Windows -con excepción de Vista, el cual aún no trabaja con el Integration Tools pero corre lento en el modo de virtualización- esto se consigue con un wizard simple y un reboot de la máquina virtual. Comencemos con los puntos a favor. En conjunto, y por lo que se pudo ver del lanzamiento del beta 1.0, Microsoft ha hecho un gran trabajo con la administración de Hyper-V: la consola de acceso al VMs es muy buena y rápida y la performance de VM es excelente. Su capacidad de administración es definitivamente mejor que las de Citrix XenServer 4.x y de las que actualmente existen en Red Hat Enterprise Linux o SuSE Linux Enterprise Server. Sin embargo, Hyper-V muestra algunas fallas en lo que a la administración de clusters se refiere, migración automática y balanceo de carga de VM ("VMotion") y capacidades HA creadas en el ESX Server 3 y VirtualCenter 3. Claro que Hyper-V es gratuito como parte del Server 2008 Standard (con una versión dedicada de $30 dólares en el camino) y ESX Server cuesta unos cuantos cientos de dólares por copia, dependiendo de las características, por lo que teniendo en cuenta el costo y la facilidad de uso, le gana a ESX.

Los puntos en contra son que solo se puede correr el administrador Hyper-V en otra máquina con Windows 2008 Server. Esto se podrá resolver una vez que el Hyper-V Manager, ahora llamado RSAT (Remote Server Administration Tools) sea lanzado para su testeo. Lo malo es que solo corre sobre Vista Service Pack (SP) 1. Parece que si se quiere optar por Server 2008 uno deberá quedarse con las conexiones Terminal Server RDP de las estaciones de trabajo XP o resignarse a tener al menos unas pocas máquinas con Vista para realizar los deberes de administrador con RSAT. Se espera que éste sea uno de los temas en lo cuales Microsoft planee trabajar, porque mientras Terminal Server es muy bueno, uno debería tener la posibilidad de administrar remotamente la consola de Virtual Machine directamente desde XP sin la necesidad de requerir de Vista u otra solución de acceso remoto como VNC o Terminal Services virtualizado.

Microsoft y Linux

Como resultado de la alianza entre Citrix y XenSource, Microsoft también brinda Integration Components para sistemas operativos Linux. Las herramientas de Hyper-V teóricamente soportarán cualquier sistema operativo Linux que incluya un kernel Xen paravirtualizado. En este momento, solo SuSE Enterprise Server 10 está soportado oficialmente, pero también se puede trabajar correctamente con el gratuito OpenSUSE 10.3 y el CentOS 5.1, un popular clon gratuito de Red Hat.

El proceso de instalación es un poco desordenado y no muy bien escrito como lo están las herramientas de VMWare -requiere de una instalación manual del kernel Xen, correr un script separado que modifique la configuración del GRUB bootloader para permitir la utilización del adaptador hypercall de Microsoft y luego correr el perl script para instalar el Integration Tools y paravirtalizar los drivers. Una vez que están instalados, la performance de Linux es excelente y comparable a lo que encontrará en un XenServer o en cualquiera de las soluciones open-source basadas en Xen. Si Microsoft liberara el Integration Components como Open Source, las distribuciones de Linux podrían brindar un paquete nativo de instalación para sus respectivas versiones para de esta forma simplificar el proceso de instalación, el cual actualmente requiere de un número de paquetes y fuentes.

Aunque aún Hyper-V está en la versión pre-1.0, Microsoft ha realizado un muy buen trabajo con su hypervisor. Mientras el ESX de VMWare es superior en una gran cantidad de frentes, incluyendo la tecnología VMotion mencionada anteriormente y su herramienta de administración de cluster sumamente poderosa, Microsoft ha superado las expectativas y ha dejado algo preocupados a los vendors de Linux. ●

El futuro de SOA gira entorno a Visual Studio, BizTalk Server, SQL Server y MSDynamics y el nombre clave utilizado por Microsoft para este set de nuevas tecnologías es "OSLO".

Microsoft® CODENAME OSLO

DANIEL M. SALAZAR

Codename: Oslo!

Las compañías lideres en Herramientas de Negocios y Tecnologías Servidor discuten acerca de cómo Microsoft simplificará significativamente el esfuerzo que requiere Diseñar, Desarrollar, Distribuir y Administrar aplicaciones distribuidas.

Microsoft acaba de completar la entrega de una emocionante ola de SOA (Service Oriented Aplications) conjuntamente con tecnologías de procesos de negocios durante 2007 con el anuncio de Biztalk Server en su última versión, .Net Framework 3.5 y Visual Studio 2008.

Microsoft está invirtiendo algunos de los mejores talentos en ingeniería de la empresa para hacer dos inversiones clave:

• Ofrecer una plataforma SOA de clase mundial a través de plataformas cliente, servidor y nubes. Microsoft ha sido desde el principio un líder de pensamiento en Servicios Web y tecnologías SOA y ha desarrollado las tecnologías líderes de la industria tales como WCF (Windows Communication Foundation) y BizTalk Server.

• Entregar un sistema de modelado que ayude a los roles de IT a colaborar y permitir mejor integración entre IT y los negocios.

La plataforma de modelado permite mejores niveles descriptivos también llamadas descripciones declarativas de la aplicación.

Este conjunto de inversiones tecnológicas unificará nuestras plataformas de modelado y servicios, moviéndonos desde un mundo donde el modelado describe la aplicación hacia un mundo donde los modelos son la aplicación.

El nombre clave utilizado para englobar todo este set de nuevas tecnologías es "OSLO".

Cruzando los límites

Robert Wahbe, Vicepresidente Corporativo de Microsoft en el área de Microsoft Server & Tool Bussiness, nos comenta los actuales desafíos y las oportunidades futuras que rodean el desarrollo de Software.

Como una introducción a las tecnologías OSLO, Wahbe comenta los desafíos que habitualmente los esfuerzos heroicos de los desarrolladores y profesionales de TI deben sobrepasar para crear una solución orientada a servicios.

Wahbe se enfoca en tres requisitos críticos que deben ser alcanzados para eliminar estos obstáculos.

Mire el video aquí:

http://download.microsoft.com/download/8/4/6/846F8EE7-46BC-47A0-A38B-3ECD8DC7EB6E/VisionforOslo.wmv

El camino hacia las Tecnologías Oslo

Wahbe marca cómo los clientes pueden comenzar a prepararse para OSLO utilizando las tecnologías ahora disponibles en BizTalk Server, BizTalk Services, Net. Framework 3.0 y Visual Studio 2005. Mientras aguardamos el 28 de Febrero el lanzamiento de las nuevas tecnologías Windows Server 2008, Visual Studio 2008, .NET Framework 3.5 y SQL Server 2008.

Estas innovaciones proveerán una base para las

"Creando un nuevo modelo de aplicaciones orientado a servicios".


FOTO: www.sxc.hu / Bensik Imeri

FOTO: www.sxc.hu / Carsten Muller

futuras generaciones de SOA y aplicaciones Web distribuidas, en algo que Microsoft llama SOFTWARE + SERVICES.

¿Qué es Service Oriented Architecture (SOA)?

Los departamentos de TI están administrando portfolios cada vez más complejos. Y a medida que los negocios necesitan cambiar, estos departamentos deben estar seguros de que sus tecnologías se mantendrán alineadas con los objetivos del negocio. Fallar en este aspecto compromete la agilidad de la organización.

Orientación a servicios es acercar los recursos distribuidos de TI organizándolos en una solución integrada que explota los silos de la información y maximiza la agilidad del negocio.

SOA modulariza los recursos de TI creando procesos de negocios asociados que integran la información en los sistemas empresariales. Cada recurso de TI, ya sea una aplicación, un sistema o interfaces, mejora cuando el proveedor de servicios difiere en cada sistema operativo, o en los protocolos de comunicación, resultando inoperativos.

SOA significa integrar diversas plataformas, usando protocolos standard e interfaces convencionales – usualmente Web Services – para facilitar el acceso a la logia de negocios (BL) y a la información entre diversos servicios.

SOA provee la guía y los principios necesarios para transformar una matriz heterogénea, compleja e inflexible de recursos TI de la empresa, en algo más integrado, simplificado y altamente flexible, que puede ser cambiado y recreado para soportar más directamente las metas del negocio.

SOA finalmente permite la entrega de una nueva generación de aplicaciones dinámicas de TI (algunas veces llamadas aplicaciones compuestas). Estas aplicaciones proveen al usuario final con información más directa y comprensiva siguiendo los procesos, como así también la forma de facilitar el acceso a la información de manera más clara y cuidando el factor presentación que trabaja directamente a través de plataformas con interfaces ricas para la Web o para dispositivos móviles.

BIZTALK SERVER

Con la introducción de BizTalk Server en 2000, Microsoft sembró una revolución en la industria de la integración, proveyendo los procesos de automatización tan costosos y difíciles de utilizar. Hoy en día, cerca de 7.000 organizaciones confían en BizTalk Server para integrar sus sistemas y automatizar los procesos en las cadenas de abastecimientos globales. Con la introducción de la quinta versión, BizTalk gira entorno al Proceso de Gerenciamiento de Negocios (BPM Business Process Management) y SOA/ESB, que permitió en versiones anteriores ayudar a las organizaciones a extender los procesos principales de gerenciamiento en tecnologías con nuevas funcionalidades, tales como soporte nativo para Intercambio Electrónico de Datos (EDI Electronic Data Interchange), AS2 y RFID. Cercanamente al lanzamiento de las nuevas tecnologías de Windows Workflow Foundation y Windows Communication Foundation.

BizTalk Server coloca en tiempo real el gerenciamiento de punta a punta de la cadena de abastecimiento con el alcance de cada cliente, distribuyendo sistemas, gente y procesos dentro

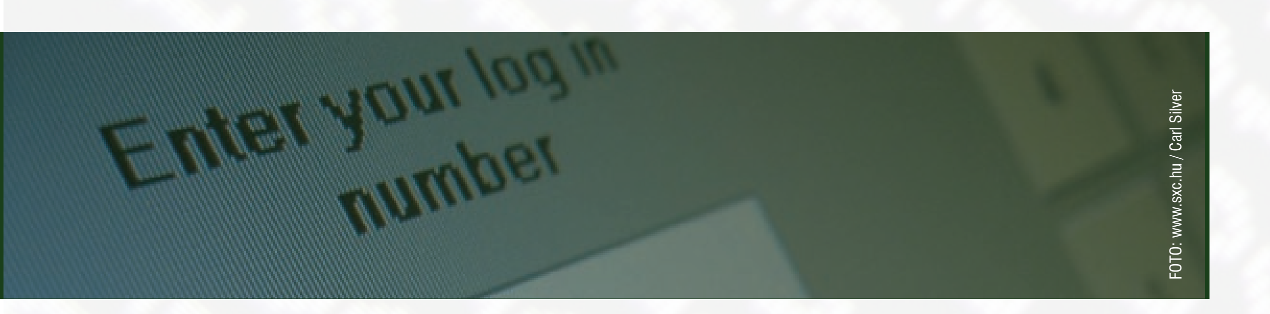


FOTO: www.sxc.hu / Carl Silver

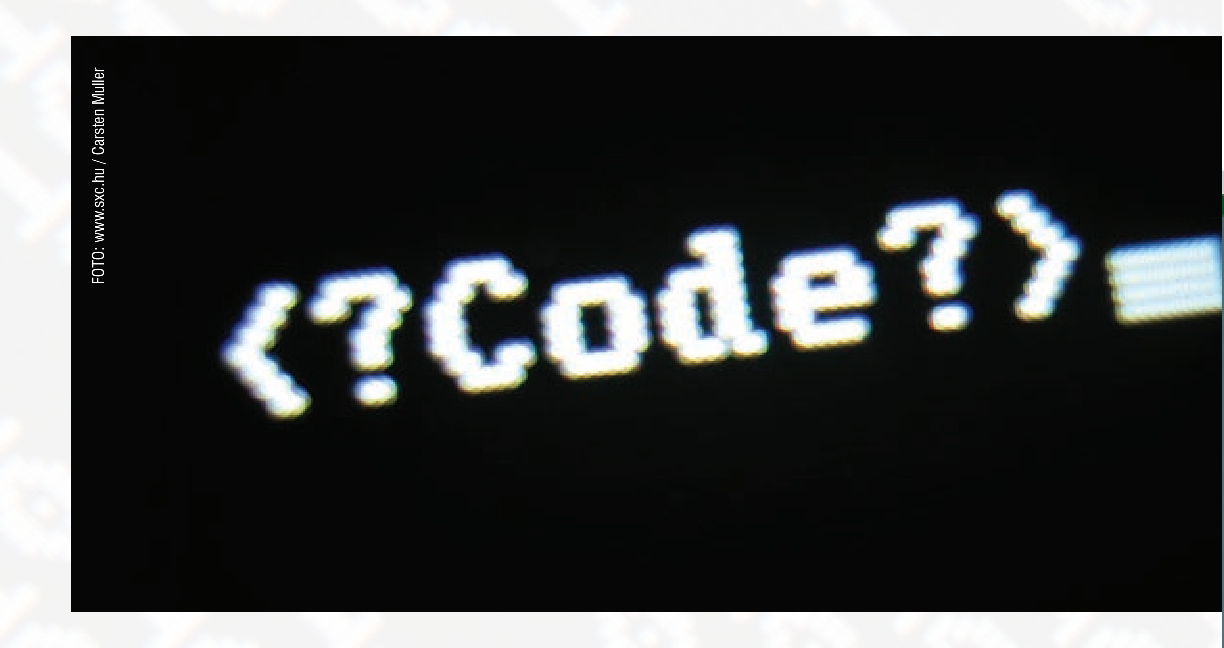


FOTO: www.sxc.hu / Carsten Muller

de la organización.

Además, potencia los clientes al ayudar a tomar decisiones de negocios importantes con datos en tiempo real de sistemas ya integrados, dispersos geográficamente, colocando al negocio un paso adelante con respecto a la competencia.
Todo esto integrado a la infraestructura de clase que brinda confidencialidad independientemente del tamaño de la organización. Su negocio, conectado.

BizTalk Server ayuda a las organizaciones a manejar de manera más efectiva los costos de la cadena de abastecimiento desde la fábrica hasta la venta.

Un manejo punta a punta de la cadena de abastecimiento brinda a las empresas la posibilidad de manejar al máximo la eficiencia visible dentro de las decisiones criticas del proceso de negocio, y dispara la colaboración entre los socios de intercambio (Trading Partners).

SOA e INTEROP en una plataforma unificada

BizTalk provee una infraestructura que permite conectarse con aplicaciones existentes (independientemente de la plataforma) y componer, exponer y consumir nuevos servicios. Esto permite sacar más provecho de las inversiones que la empresa ya realizó y minimizar así los costos de integrar nuevas piezas a la tecnología ya adquirida. Debido a que BizTalk Server incluye herramientas para conectarse en forma propietaria, sistemas standard base y preintegrados con .Net Framework, BizTalk es parte integral de cualquier estrategia de SOA.
Adicionalmente, un sinfín de tecnologías y adaptadores para aplicaciones están disponibles para BizTalk Server. Con todo esto plus el soporte para casi todo protocolo de transporte, tales como FTP, SOAP y MQSeries, hasta un alto nivel de integración con la línea de aplicaciones de negocios tales como PeopleSoft, SAP, y Siebel, le permiten elegir sobre cómo quiere Usted conectar sus aplicaciones, plataformas y personas.

BizTalk le provee las herramientas para efectuarlo.

- Línea de adaptadores para aplicaciones de negocios
- Standard Base par Web Services
- Net Framework (WCF, Windows SharePoint Services, SQL Server, Microsoft Dynamics, etc)
- Sistemas Mainframe y Midrange.
- Protocolos WS y XML (ej. SOAP)
- Dispositivos (RFID)
- Para ver una lista completa de adaptadores vea http://www.microsoft.com/biztalk/evaluation/adapter/default.mspx

Acerca del Autor



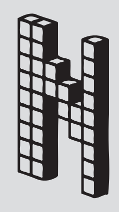
Daniel Salazar
MCP – MCTS - New Technologies Evangelist
Oxford´s University FCIC
Microsoft Senior Trainer

Oslo es un conjunto de inversiones tecnológicas que unificará nuestras plataformas de modelado y servicios, moviéndonos desde un mundo donde el modelado describe la aplicación hacia un mundo donde los modelados SON la aplicación.

Federico Nan

NO AL SPAM CON LINUX

FOTO: www.sxc.hu / Rodolfo Clix


o es ninguna novedad que el Correo Solicitado o SPAM es parte de nuestra vida diaria. Muchos de nosotros agregamos a nuestra rutina el borrar correo basura de nuestras casillas. El porcentaje de acierto de esos correos con nuestras necesidades es muy bajo, casi nulo. No conozco a nadie, incluyendo amigos de sistemas y usuarios de empresas para las que trabajo, que me haya dicho alguna vez que compro algún producto o servicio por un correo que llegó como propaganda.

En las empresas, la guerra contra el SPAM cada vez es más fuerte. Estos correos generan un malestar en lo usuarios, y por consiguiente en la gente de sistemas; así como también, una pérdida de performance en el enlace y los recursos del servidor de correo.

Mi idea en este artículo, es entregarles algunos recursos teóricos y prácticos para enfrentar a nuestro enemigo el SPAM.

El enfoque que propongo siempre está basado en el uso de herramientas Open Source. Son muy flexibles, escalables y estables. La documentación alrededor de ellas es mucha. Por lo tanto, el soporte que tenemos es amplio y siempre podemos encontrar una solución enfocada a la problemática de la empresa.



Conceptos Básicos

Dividí el artículo en 3 apartados. El primero con conceptos básicos. El segundo, el protocolo ESMTP. Y por último analizaremos una solución antispam Open Source.Alguna terminología para tener a mano. ¡Siempre es bueno recordar qué significa cada cosa!

ESMTP: Es el protocolo SMTP extendido. Esta mejora que se implementó sobre este viejo protocolo permitió que el envío del correo sea un poco más seguro y eficiente. Proporcionó, por ejemplo SMTP AUTH o autenticación de envío de correos. Con esta mejora los usuarios deben autenticarse con un nombre de usuario y contraseña para poder usar el servidor de correo. Los métodos de SMTP AUTH más conocidos son: PLAIN (el usuario y la contraseña se envían en texto plano al servidor), MD5 (el usuario y la contraseña son encriptados), NTLMv2 y GSSAPI (métodos de autenticación de Microsoft), utilizados para hacer single sign-on en ambientes Active Directory.

La aplicación más conocida de autenticación que se usa en servidores de correo en Linux se llama SASL, que soporta todos los métodos mencionados anteriormente. Otro valor agregado en esta implementación fue la de poder entregar a los clientes una conexión totalmente encriptada sobre TLS (Transport Layer Security). De esta manera, los correos viajan encriptados desde el cliente hasta el servidor.

UCE: (Unsolicited commercial e-mail) Correo comercial no solicitado, o simplemente, otra manera de llamar al spam. Los proyectos importantes de servidores de correo, en su documentación, tienen un apartado para Anti-Uce. Varias técnicas pueden aplicarse para detectar este tipo de correos sin la necesidad de un programa adicional anti-spam. Estos métodos son llamados por algunos desarrollos como Sanity Checks.

OPEN RELAY: Un servidor de correo bien configurado solo permite enviar correo a usuarios autenticados o que pertenezca a sus redes de confianza. Cuando esto no sucede, el servidor permite el envío de correo a cualquiera. En Internet hay muchos open relays. Muchos de estos suelen enviar spam.

Uno de los mayores problemas que surgen en las empresas es que, por no tener conocimiento, sus servidores de correo son utilizados para el envío de correo no solicitado. Este tipo de envíos masivos sobrecargan el enlace y el servidor de correo.

RBL: Real-time Blackhole List. Este término forma parte de un proyecto mayor llamado DNSBL. La finalidad de este software que se instala en los servidores de correo es la de bloquear spam.

Las IP de los servidores de correo Open Relay o que presenten algún indicio de envío de spam se colocan en listas para que nuestro MTA consulte cada vez que un correo llega. Hay muchas listas en Internet, algunas libres y otras pagas.



Enviando correo con ESMTP

Para corroborar que un correo es de la persona que dice ser, hay varios chequeos que podemos realizar antes de que el mensaje termine de enviarse. Cuando se envía un correo, el servidor de origen debe presentarse al de destino. Vamos a recorrer una sesión telnet de envío de correo y ver por pasos algunos de los chequeos que podemos hacer.

El primer paso es conectarse al servidor destino y presentarnos. En este punto, un servidor bien configurado se presentará con su nombre FQDN válido, por ejemplo mail.dominio.com.ar. Este FQDN tiene que tener en su DNS un registro PTR (consulta reversa). Es muy probable que los servidores que envían spam no cumplan esta función.

En este punto también las RBLs entran en acción, chequeando el nombre en las listas a las que estemos adheridos.

telnet mail.linux.com 25 (este es el servidor de destino)
ehlo mail.dominio.com (habilitamos la charla ESMTP y nos presentamos con nuestro nombre verdadero)
250-mail.linux.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN NTLM GSSAPI
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN

Luego de la presentación, el servidor nos muestra cuáles son las opciones que soporta. Si el nombre proporcionado en el ehlo, no es correcto, entonces el servidor nos rechazará la conexión. Según su configuración, algunos servidores pueden enviar un correo de rechazo informando que nuestro equipo está en una lista RBL, o simplemente está mal configurado.

Este proceso lo hace el MTA, realizando una consulta reversa al dominio FQDN proporcionado en el comando ehlo.

Cuando trabajamos con software libre, la cantidad de opciones que tenemos son muchas. Con las RBLs, pasa lo mismo. Por eso es muy importante conocer bien cada una. Hay que tener en cuenta que, a veces, puede ocurrir algún falso positivo si nosotros ponemos alguna lista que sea muy restrictiva.

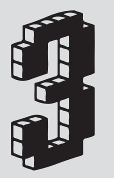
Algunas de las más conocidas son:
http://www.spamhaus.org
http://www.spamcop.net
http://relays.ordb.org

Las listas mencionadas son muy efectivas. Por lo general, reflejan la verdad y es muy raro que surja algún falso positivo.

También, nuestro servidor de correo puede chequear que el mail que está llegando esté armado siguiendo las RFC. En muchos casos los programas encargados de enviar spam no siguen esta reglamentación. Es otro buen paso para filtrar correo no deseado.

Es importante configurar en nuestro servidor el uso de estas normas. A mi parecer, el mejor servidor de correo para realizar estas tareas es Postfix. Su potencia y estabilidad hacen que pueda soportar mucha carga de correo. Posee todas las opciones para poder hacer un primer buen filtrado de correo basura. El proyecto está muy bien documentado, y los usuarios en las listas de correo están listos para contestar nuestras dudas.

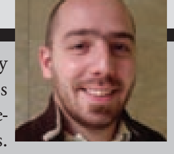
Podemos complementar todo este sistema, con una buena herramienta como el spamassassin para terminar de eliminar el spam.



Matar el spam con spamassassin y amavisd

Ya vimos que hay varias maneras de comenzar a eliminar el spam. Las RBLs son una buena opción; también los sanity cheks, que nuestro servidor de correo puede hacer sobre cada e-mail que llega.
Si el correo fue capaz de superar estas pruebas podemos utilizar otra herramienta llamada Spamassassin. Esta herramienta es un conjunto de poderosos escaneos sobre los emails. Posee un sistema de aprendizaje para que nosotros podamos entrenarlo con el paso del tiempo. De esta manera, podemos llegar a un 99 por ciento de aciertos en el escaneo. Como toda implementación tiene una contra.: por la cantidad de escaneos que realiza suele ocupar muchos recursos del servidor. En grandes implementaciones es recomendable utilizarlo en un servidor separado del de correo.
Otra herramienta muy útil es Amavisd. Ésta nos proporciona la misma funcionalidad pero sin consumir tantos recursos. Hay muchos proyectos open source alrededor de esta herramienta para facilitar su manejo. Amavisd usa parte de Spamassassin.
La guerra contra el spam es una tarea difícil, que lleva dedicación y tiempo. Pero no es imposible. El mundo open source proporciona todas las herramientas necesarias para esta lucha. Podemos encontrar mucha documentación en Internet, en la página de cada proyecto. Les dejo los links que considero más importantes, así como también algunas páginas para configurar un buen servidor anti-spam. •

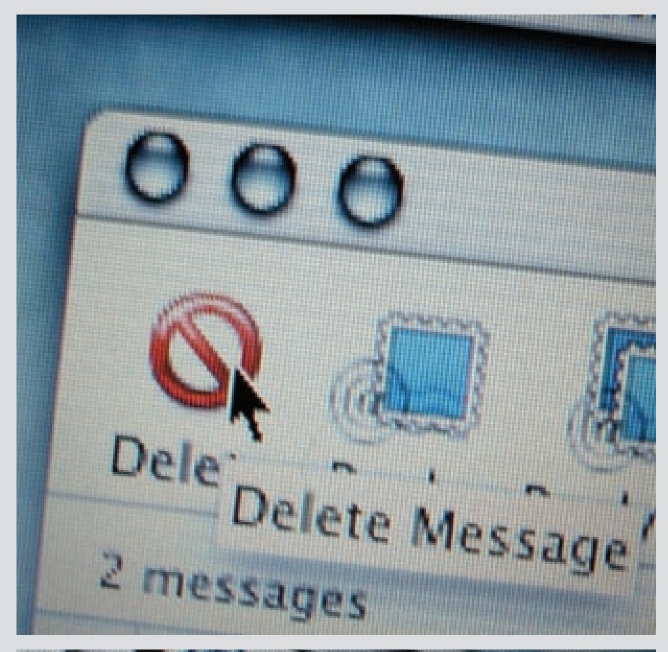
Acerca del Autor

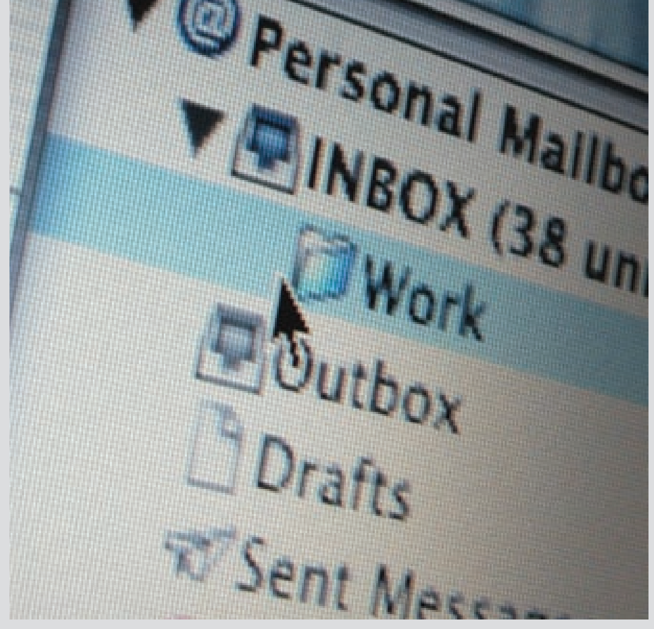


Federico Nan comenzó su trabajo en Unix y GNU/Linux en el año 2000. En la actualidad es consultor en plataformas GNU/Linux. Se especializa en soluciones de correo y comunicaciones. Desde Nantec.net, su empresa, brinda soluciones a medianas y grandes empresas junto a un grupo de jovenes consultores.

Links recomendados y lectura adicional

http://spamassassin.apache.org/
http://www.posluns.com/guides/
http://www.postfix.org
http://www.ijs.si/software/amavisd/
http://www.mob.net/~ted/tools/rbl.php3





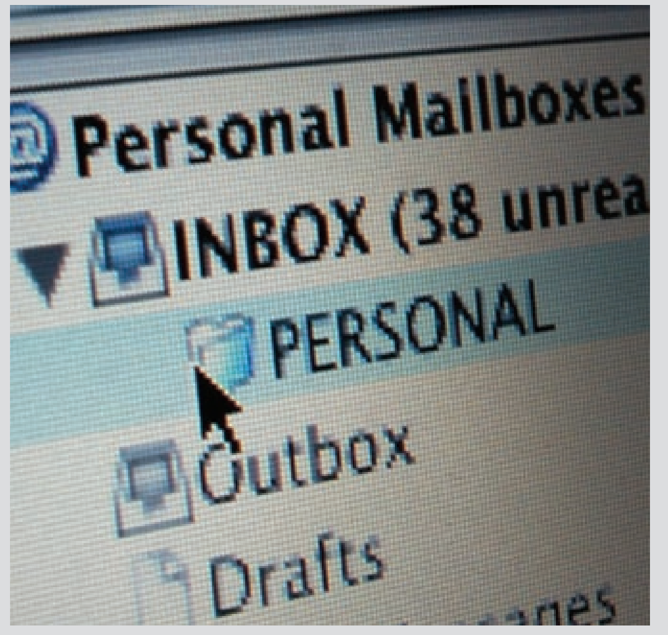


FOTO: www.sxc.hu / Dan Mulligan

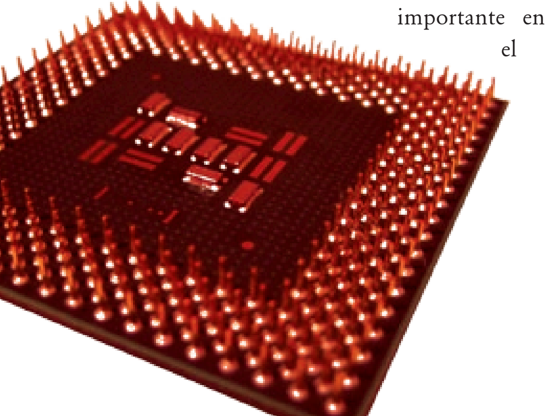
Hacer posible el hardware abierto

Alicia Asín Pérez es una ingeniera informática española, fundadora de la empresa Libelilum, dedicada al desarrollo de redes distribuidas sensorialmente, responsable de proyectos tales como SquidBee y Arduino, y ganadora de varios premios a la innovación y por el proyecto de empresa desarrollado. Pero además es una de las promotoras de un nuevo movimiento, un nombre que esta empezando a sonar fuerte en el ambiente de las Tecnologías de la Información y la Comunicación, Open Hardware.

FOTO: www.sxc.hu / dima v

A partir de un artículo escrito por ella para el sitio Free Software Magazine, nos comenzó a rondar en la cabeza la siguiente pregunta ¿Hardware Abierto? ¿De qué están hablando?. Sin dudas que el modelo de Software Libre, más allá de las eternas polémicas con el software de código cerrado, tiene amplios beneficios.

Se puede obtener software más seguro, rápidas actualizaciones y definitivamente representa una nueva forma de hacer software, basada en las comunidades y en donde todos tienen a su disposición el código utilizado para poder participar activamente, crear y aportar a los nuevos desarrollos. Este modelo, con altibajos como todos, es cierto, ha logrado ganar un lugar muy importante en el mundo de las ICT, es cada vez más exitoso y se encuentra totalmente asentado. El siguiente paso lógicamente es el de llevar esa estructura abierta también al Hardware y aunque de entrada suene a utopía difícil de realizar lo cierto es que ya existe una creciente comunidad dispuesta a desarrollar Hardware Abierto. El Software Libre se basa en cuatro libertades fundamentales: libertad para ejecutar programas, libertad para acceder al código fuente, libertad de distribuir copias y libertad de mejorar y hacer públicas las modificaciones. Sin embargo la cuestión no es tan sencilla como trasladar el modelo de Software Libre al mundo del Hardware.



Si nos remontamos a la historia de la informática nos damos cuenta que el concepto de Hardware Abierto es casi tan viejo como el de Software Libre. En los años 70 en pequeños grupos de programadores y universitarios ya se empezaba a hablar del tema. Sin embargo, al tratarse de una idea no tan práctica como la de liberar programas, hasta el momento no se ha llevado a cabo. De hecho el mismo Richard Stallman, figura más relevante del movimiento de Software Libre, ha declarado en más de una ocasión que es mejor concentrarse en el software, porque hacer posible un movimiento de Hardware Libre es una tarea casi imposible. No obstante pequeñas comunidades empiezan a no aceptar esos imposibles y comienzan a trabajar para revertir la situación.

Desde el vamos, hardware y software pertenecen a universos paralelos. Las cuestiones relativas al software son gobernadas por el derecho de autor, mientras que las invenciones que implican equipos físicos son protegidas por patentes. Sin embargo la diferencia fundamental es que el hardware inevitablemente implica otros costos de componentes y fabricación. Hacer copias y distribuirlas gratuitamente por lo tanto es infinitamente más complicado que en el caso del software.

Por eso quienes hoy trabajan en comunidad para desarrollar este nuevo concepto, tienen una difícil pero no imposible tarea por delante. Hoy existe una iniciativa denominada Certificación de Hardware Abierto, y es un programa de certificación libre para fabricantes de hardware. Se trata básicamente de que



cuando alguien certifica un nuevo dispositivo como Hardware Abierto se compromete a poner disponible la información competente, suficiente como para que cualquier técnico, programador o ingeniero con la pericia y los medios necesarios pueda escribir un controlador del dispositivo. La documentación debe cubrir todas las características de la interfaz del dispositivo-controlador que se esperaba que cualquier usuario empleara.

Los componentes del hardware que se pueden liberar son por ejemplo el Firmware, esquemas, diseño de circuitos y diagramas, listados, entre otros. Así en el sitio www.opencircuits.com se pueden encontrar cada vez más proyectos de Hardware Abierto. Lo que esta certificación propone es que por ejemplo si alguien desarrolló un nuevo dispositivo en Tokio y decide liberar la información, otra persona en Buenos Aires 10 minutos más tarde pueda hacer una impresión esquemática con los principales circuitos del dispositivo, para poder copiarlo. Pero para que esto sea posible, quién cree un nuevo artefacto con la idea de patentarlo como Open Hardware debe fabricarlo con componentes comunes, baratos y estándar. La estandarización internacional para intercambiar diseños y que estos sean legibles para todo el mundo es fundamental. El prototipo de plataforma Arduino es un buen ejemplo de todo esto. Se puede programar para leer sensores, control de motores y construcción de objetos interactivos e instalaciones artísticas. Su compilación de medio ambiente es multiplataforma y libre y el único extra de hardware necesario para la programación se trata de un serial/cable USB. Este software se puede descargar de la página Web Arduino.

Otro de los temas sensibles es el de las licencias. El hardware debe ser protegido por una patente y estas tardan mucho tiempo y son costosas, por lo que resulta muy difícil costearla. Por eso hay varios lanzamientos para proteger los proyectos de Hardware Abierto a través de licencias Creative Commons además de la propuesta de la organización TAPR, de otorgar licencias OHL, una alternativa al GPL que se utiliza en el software.

A pesar de las grandes dificultades que conlleva implementar un modelo de Hardware Abierto, también puede otorgar grandes beneficios. Uno de los principales es que les daría a los usuarios independencia de elección y otro es que se achicarían las grandes brechas de conocimiento que existen entre países, regiones y grupos sociales. Además los productos podrían ser mejorados por comunidades enteras, logrando así las compañías ahorrar dinero invertido en diseño, ya que la comunidad se encargaría de ello y de manera gratuita. El único requisito que debería cumplir quienes quisiesen comercializar Hardware Abierto es el de mantener esa libertad de información, ponerla disponible para quien quiera utilizarla.

Pensar en verde

Más allá de que se trate del concepto de moda en el mundo de la tecnología, Green IT puede ser una gran oportunidad para las compañías para ahorrar dinero y para ayudar a cuidar nuestro castigado planeta.

En la era del cambio climático y calentamiento global, desde hace un tiempo se vienen sucediendo noticias de que todos y cada uno de los grandes vendors de la industria apuestan por tecnologías verdes. Y es que más allá de las lógicas preocupaciones por el cuidado del medio ambiente, algo que afecta no solo a la industria IT sino a todos los sectores económicos, existen otras poderosas razones.

A diferencia de lo que se podría pensar a priori, Green IT no se trata de solamente de pensar en acciones que ayuden a reducir el impacto ambiental que generan la producción y el uso de las nuevas tecnologías sino que se trata de una gran posibilidad para la industria de ahorrar costos y optimizar la eficiencia en el uso de energía.

Pero, ¿qué se significa exactamente Green IT?

La computación o informática verde no es un concepto nuevo, pero sí lo es el boom que existe alrededor del tema. Se trata básicamente de la búsqueda de reducir el uso de materiales peligrosos en la manufacturación de los productos, del reciclaje de los mismos y de la optimización del uso de la energía que es necesaria para que funcionen las nuevas tecnologías.

Intel, Microsoft, HP, Sun, AMD, VMware, IBM y Dell, entre otros, han hecho punta en la nueva tendencia e incluso son socios en Green Grid, una organización dedicada a avanzar hacia un uso eficiente de la energía, en especial en los data centers.

Los Centro de Datos son el lugar clave para el ahorro de energía en las empresas IT. Y en ese escenario resulta vital la implementación de otro de los temas más “calientes” de la actualidad: la virtualización. A través de la virtualización de servidores se reduce el espacio físico, la cantidad de componentes a alimentar y sobre todo se reduce el gasto de enfriamiento.

Los aires acondicionados de los Data Center son los principales responsables de gasto de energía ya que representan el 50 por ciento de la energía utilizada en los mismos. Se calcula que a través de la virtualización se puede lograr un ahorro de hasta un 90 por ciento en los servidores. Además, los servidores virtuales pueden trasladarse o replicarse con mucha facilidad y permiten la recuperación en casos de desastres. Por algo la virtualización parece ser uno de los sectores más prometedores de la industria y Microsoft parece dispuesto a pelearle el mercado a los líderes VMware.

Las grandes empresas tecnológicas, más allá de Grid Green, luchan día a día por ser "la empresa más verde" del mercado. Ser una "empresa verde" significa aportar a la conservación del medio ambiente, posicionarse como una compañía con responsabilidad social y conciencia ambiental y ahorrar energía y, por ende, dinero.
IBM a través de su proyecto Big Green, lanzado a fines de 2007, invirtió 1.000 millones de dólares en el desarrollo de nuevos productos que respeten los principios del Green IT.

En junio de 2007 Google e Intel lideraron un grupo de compañías que se unieron para lanzar "The Climate Savers Computing Initiative", una iniciativa destinada a fomentar el ahorro de electricidad y reducir las emisiones contaminantes a través de la fabricación de equipos informáticos y servidores con mayor eficiencia energética.

Dell ha creado una serie de productos de desktop y portátiles que consumen menos de 5 vatios en el modo de baja potencia.

El Service Pack 1 de Windows Vista traerá una serie de mejoras para ayudar en el ahorro de energía y a través del lanzamiento de la plataforma de virtualización que vendrá dentro del Windows Server 2008, la compañía de Redmond apunta a que sus usuarios logren ahorrar grandes cantidades de energía.

Apple ha reciclado, según sus funcionarios, más de 13 millones de libras de desechos electrónicos solo en 2006, mientras que en 2007 esa cifra fue mejorada en un 13 por ciento, además de haber eliminado el plomo de sus baterías.

AMD a través de su procesador de cuatro núcleos a logrado duplicar la potencia del procesador de dos núcleos pero utilizando la misma cantidad de energía y la misma térmica.
Intel se ha convertido recientemente en la empresa número uno en consumo de energía renovable y se ha unido a la comunidad Linux en varios proyectos para ahorrar energía a través de la utilización de procesadores multi-core en plataformas Linux.

Por su parte, la consultora IDC ha creado un departamento de investigación llamado IDC Green, especializado en analizar las ofertas de servicios y proveedores verdes. Y un informe de este departamento señala que más del 50 por ciento de los clientes tienen en cuenta el compromiso con la energía verde a la hora de elegir un proveedor y más del 80 por ciento de los ejecutivos IT consideran que el Green IT está creciendo en importancia para sus organizaciones.

Uno de los primeros pasos que se pueden dar para ingresar al mundo Green IT es consultar la página de EPEAT (Electronic Product Environmental Assessment Tool: www.epeat.net) antes de actualizar computadoras o servidores, ya que allí se encuentra la información sobre qué productos y compañías respetan procedimientos que apuestan por el cuidado del medio ambiente y el ahorro de energía.


FOTO: www.sxc.hu / xlucas's

¿Está su perfil en demanda?

Estar actualizado en la última tecnología le puede abrir nuevas y mejores oportunidades laborales, ayudarlo a avanzar en su organización y recibir como compensación un muy buen salario. Pero, ¿en qué lugar de importancia se encuentra su expertise en IT? NEX IT Specialist junto a CentralTECH (Capacitación Informática) hemos elaborado un ranking de los perfiles más buscado del mundo TICs.

En IT, como en otras profesiones, lo más importante son las habilidades. Mantenerse actualizado abre puertas, nos brinda nuevas oportunidades y nos ofrece un panorama laboral realmente atractivo. Por eso resulta fundamental conocer qué perfiles son los más buscados para enfocarse en ellos.

Desarrolladores/Diseñadores Web

Mientras las empresas aumenten su inversión en aplicaciones e iniciativas Web, los profesionales con habilidades en desarrollo y diseño serán uno de los más buscados. De hecho, los candidatos con estas habilidades ganan un 10 por ciento más por salario que aquellos que no las poseen. Conocimientos en .NET y Java es sumamente valorado para posiciones de desarrolladores o diseñadores Web y desarrolladores de software o ingenieros.

SQL Server y MySQL

El crecimiento de aplicaciones y desarrollo Web también influye en la necesidad de habilidades en SQL Server y MySQL. Las empresas necesitan profesionales que sepan escribir código, incluyendo procedimientos de almacenamiento, scripts de bases de datos y triggers.

Administración de Windows

¿Es muy bueno con Windows Server 2003 o XP? ¿Tiene experiencia con Active Directory? Si es así, este es su momento. Los conocimientos en administración de Windows es una de las habilidades técnicas que más demandan los departamentos de IT. Es muy valorado en posiciones como administrador de sistemas, analista de soporte y administrador de mesa de ayuda. Todos aquellos que pueden instalar, configurar, administrar y mantener un servidor Windows ganan aproximadamente un 10 por ciento más que aquellos candidatos sin este conocimiento.

Administración de Redes

Las habilidades en administración de redes son muy buscadas, particularmente aquellos con experiencia en redes Cisco. Ingenieros de redes, administradores de sistemas y de telecomunicaciones son las posiciones que generalmente requieren del mantenimiento y la solución de problemas de routers de Cisco, hubs y switches. Estos profesionales suelen ganar un 12 por ciento más que aquellos que no cuentan con este conocimiento. Además, muchas empresas le dan importancia a las certificaciones asociadas con el tema y como plus la experiencia en seguridad de redes.

Administrador de Bases de Datos

En la actualidad cada vez se reconoce más la importancia de mantener la información ordenada y segura, por lo que se necesita profesionales con las habilidades para lograr estos objetivos. Los conocimientos más valorados son los referidos a bases de datos Oracle, Microsoft SQL Server y MySQL, por lo que aquellos con esta habilidad ganan un 10 por ciento más que aquellos que no la poseen. Los conocimientos en administración de base de datos son necesarios para poder manejar eficazmente todo desde la implementación a la actualización y al análisis de la información.

Wireless Network Management

Los dispositivos wireless, tales como las tablet PCs, lso smartphones y las laptops se han vuelto cada vez más comunes dentro del ambiente de trabajo, y esto se corresponde con la creciente necesidad de profesionales con conocimientos en administración de redes wireless.

Puestos de trabajo como administradores de mensajes e ingenieros de redes son quienes ayudan a que las organizaciones mantengan a su equipo y a sus clientes conectados. Los conocimientos en administración de redes wireless son fundamentales para asegurar la compatibilidad de los productos con la infraestructura de seguridad y de red de la empresa en cuestión.

Ya es algo conocido que la industria de IT está en real crecimiento en nuestro país. Y para que esta tendencia continúe se necesita de profesionales que acompañen este crecimiento. Por lo tanto, los profesionales con estos conocimientos y habilidades no solo pueden esperar un crecimiento de sus salarios sino la inclusión de bonus especiales e incentivos a la hora de recibir ofertas laborales.

Hay una gran competencia por aquellos con conocimientos especificos, por tanto perfeccionarse en alguna de estas es un muy buen camino: la recompensa es grande y llega rápido.

FOTO: www.sxc.hu / Svilen Milev

El futuro tecnológico de Microsoft

Imagen 1 - LucidTouch: Conozca a LucidTouch, una pantalla táctil y traslúcida para dispositivos móviles. Permite que las personas interactúen con el contenido de la pantalla tocando la parte de atrás del dispositivo. Este efecto de seudo transparencia fue creado para sentir la mano e interpretar su ubicación en la pantalla.

Si Microsoft Research es la muestra más clara del compromiso de la compañía de Redmond por competir en la carrera tecnológica, TechFest es su plasmación más real; un evento celebrado una vez al año, en el que los investigadores de Microsoft Research muestran sus avances anticipando en pequeñas dosis el futuro tecnológico más inmediato. Su objetivo: identificar las sinergias entre MSR y los Grupos de Producto con el fin de incorporar innovaciones y mejoras a los productos de la compañía.

Actualmente, Microsoft Research trabaja en más de cuarenta áreas de investigación diferentes, que van desde el desarrollo de software para el reconocimiento de idiomas o la investigación sobre la interfaz de usuario, hasta proyectos sobre procesadores de lenguaje natural. Tanta diversificación hace necesario que el equipo de trabajo, compuesto por más de 600 investigadores procedentes de los cinco continentes, participe y colabore de una cultura común que permita aprovechar todo ese saber de una forma conjunta. Y eso es exactamente TechFest, un foro donde los científicos e ingenieros de Microsoft Research someten sus investigaciones al criterio del resto de científicos, provocando, además, el trabajo codo con codo con los grupos de desarrollo de productos. Una de las presentaciones más imponentes fue la del WorldWide Telescope (WWT), la cual da la sensación de tener el planetario pero en la PC. Permite a la gente encender su PC para convertirla en uno de los más potentes telescopios del mundo con

Dispositivos gráficos de alta resolución, claves visuales de seguridad, ordenadores cada vez más humanos... Microsoft muestra el futuro tecnológico más inmediato en TechFest.

base en la tierra. La tecnología recurre a decenas de millones de imágenes digitales de estrellas, galaxias y quásares obtenidas de Sloan Digital Sky Survey, un ambicioso proyecto astronómico que dio inicio hace varios años para crear planos de una gran parte del universo. Sin embargo y hasta el momento, era difícil buscar las imágenes. “Lo que hemos hecho es dar a la gente la capacidad de convertirse en astronautas digitales”, afirmó Rick Rashid, vicepresidente ejecutivo de Microsoft Research. “Los usuarios pueden explorar las entrañas del espacio desde la comodidad de su sala.” Los investigadores planean agregar narraciones integrales a las imágenes para crear experiencias de aprendizaje completas. “Estas experiencias equivaldrán a los recorridos guiados acerca del universo”, comentó Rashid. “La gente contará con una excelente forma para buscar, explorar y descubrir el universo de una forma muy parecida a MSN Virtual Earth”, explicó.



Imagen 3 - Video Collage
Xian-Sheng Hua, investigador de Microsoft Research Asia, muestra el Video Collage, el cual sintetiza automáticamente las imágenes para resumir el contenido de un video.

En realidad, este telescopio es una extensión de un proyecto original desarrollado por Jim Gray, el investigador de Microsoft que se perdió en la costa de San Francisco hace un año atrás (puede leer más acerca de Gray en NEX #34). Otros proyectos, más cercanos a la Tierra, se presentaron en el TechFest. Por ejemplo, un grupo de investigadores desarrolló un plug-in para el Internet explorer el cual permite guardar los resultados de las búsquedas y compartir notas a través de diferentes locaciones. ●

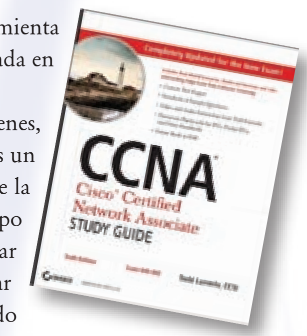
Imagen 2 - Trident
Keith Grochow de la Universidad de Washington junto a Jared Jacksaon de Microsoft Research Redmond muestran el proyector Trident, diseñado para proveer de un volumen de trabajo para los oceanógrafos.

Image 4 - WorldWide Telescope
Esta es una de las tecnologías más avanzadas presentadas durante el TechFest 2008. El WorldWide Telescope (WWT) da la sensación de tener el planetario pero en nuestra propia PC.



La Cisco Certified Network Associate, CCNA, es una de las certificaciones más populares y requeridas del mercado. La misma es otorgada por el gigante de la redes a quienes hayan demostrado a través de exámenes internacionales, que son capaces de instalar, configurar, operar y solucionar problemas de mediano tamaño de enrutamiento y conmutación de las redes, incluida la aplicación y verificación de las conexiones a sitios remotos en una WAN. Se trata sin dudas de una de las certificaciones iniciales más buscadas por la industria. Quien posee una certificación CCNA, es visto por el mercado como un experto capaz de dar soporte técnico y administrar sistemas de redes. El prestigio que tiene está certificación proviene en parte de lo exigente que son los exámenes. Para aprobarlos es necesario demostrar un buen nivel de conocimiento en varias áreas, como la configuración de routers y switches Cisco, un gran conocimiento del modelo OSI de siete capas, así como también de varios protocolos de enrutamiento tales como RIP, IGRP, EIGRP, OSPF, entre otros. Aquí algunos de los mejores libros que lo ayudaran a preparar los exigentes exámenes de certificación.

CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802 *(Todd Lammle)*



Tal como su nombre la indica este libro apunta a la preparación de CCNA, 640 - 802. Se trata de una importante herramienta para preparar exámenes ya que viene a cubrir todas las actualizaciones incluidas en la última versión del examen lanzada en agosto del años pasado, tales como seguridad, wireless, IPv6, entre otros.

El libro de Todd Lammle permite evaluar los conocimientos, conocer los conceptos claves que se toman en los exámenes, viene con CD ROM que permite practicar con cientos de posibles preguntas de examen en tiempo de examen real, más un video de capacitación de una hora que trata los temas más complejos y que no se pueden explicar bien solo a través de la escritura. Además uno de los puntos más destacados es que viene con una especie de guía, para calcular cuanto tiempo dedicarle durante los exámenes a cada sección, algo muy útil que muchos de los que han estado rindiendo sabrán valorar muy bien. Muy útil también resulta el capitulo que otorga herramientas y recursos para ayudarle al estudiante a crear su plan de estudios final. Por algo su autor posee fama mundial, gracias a los más de 25 años de experiencia trabajando con redes LAN y WAN y brindando conferencias sobre ello alrededor del mundo.

CCNA Official Exam Certification Library CCNA Exam 640-802 *(Wendel Odom)*

Wendel Odom es el autor que más libros ha vendido sobre el tema de certificaciones. Y presenta una guía pensada para rendir el exámen 640 - 802, para ayudar y aconsejar a los aspirantes y hacerles más fácil ese importante paso. Se trata del libro más vendidos de todos los existen sobre certificación CCNA.

Esta guía le ayudara a dominar absolutamente todos los aspectos que conciernen a la certificación CCNA, incluyendo: * TCP / IP y OSI - * Operativo de Cisco routers y switches LAN - * Conmutador Ethernet de configuración y solución de problemas - * LAN virtuales - * Wireless LAN - * Direccionamiento IP y subnetting - * Protocolos de enrutamiento - * Router de configuración y solución de problemas - * IP listas de control de acceso - * OSPF y EIGRP configuración - * WAN configuración y solución de problemas - * Red de Seguridad y VPNs - * NAT - * IPv6 - * Solución de problemas. El autor trabaja en la industria desde 1981 y desde hace más de catorce años dicta cursos autorizados de Cisco.



CCNA Video Mentor: CCNA Exam 640-802



Más de cuatro horas de instrucción visual personalizada con Wendell Odom, puede ser otra buena opción a la hora de prepara los exámenes. El DVD contiene un total de 20 videos, cada uno de los cuales lo guiara a través de las tareas de configuración esencial para la CCNA, incluidos router, subnetting, IP, IPv6, VLANs. Este producto es parte de la serie Video Mentor creado por Cisco, la cual apunta a cerrar la brecha que hay entre conocimientos conceptuales y aquellos de aplicación práctica.





Linux academy

```
# ls -l /dev/hda

               .88888888:.
              88888888.88888.
            .8888888888888888.
            888888888888888888
            88' _`88'_  `88888
            88 88 88 88  88888
            88_88_::_88_:88888
            88:::,::,:::::8888
            88`::::::::::'`8888
           .88  `::::'    8:88.
          8888            `8:888.
        .8888'             `888888.
       .8888:..  .::.  ...:'8888888:.
      .8888.'     :'     `'::`88:88888
     .8888        '         `.888:8888.
    888:8         .           888:88888
  .888:88        .:           888:88888:
  8888888.       ::           88:888888
  `.::.888.      ::          .88888888
 .::::::.888.    ::         :::`8888'.:.
::::::::::.888   '         .::::::::::::
::::::::::::.8    '      .:8::::::::::::.
.::::::::::::::.        .:888:::::::::::::
:::::::::::::::88:.__..:88888:::::::::::'
 `'.:::::::::::88888888888.88:::::::::'
       `':::_:' -- '' -'-' `':_::::'`

# passwd [CentralTECH]

CentralTECH:heJuwMrBVa6mg:1001:202:Academia Linux:/home/CT:/bin/sh

# useradd -u 500 -d /home/CentralTECH -G floppy,pppusers,popusers CentralTECH
```

Linux es el sistema operativo **open source** por excelencia que todo profesional debe conocer. Elegido por miles de empresas. Reconocido por miles de usuarios. Con gran Valor Agregado, Excelente Performance, demostrada Seguridad y Alta Confiabilidad. **CentralTECH** brinda capacitación y Servicios de Consultoría bajo la Plataforma Linux.



http://centraltech.com.ar - Av. Corrientes 531 - Piso 1 // Viamonte 577 - Piso 2 - Buenos Aires - Argentina







EMPRESAS/ESTADO
Teléfono: 5277.2801
http://www.centraltech.com.ar/empre-promos.asp

ESTUDIANTES PARTICULARES
Teléfono: 5031.2233/34
http://www.centraltech.com.ar/estu-promos.asp

CAPACITACION A DISTANCIA
Teléfono: 5031.2233/34
http://www.centraltech.com.ar/dist-promos.asp

NOTICIAS EN EL MUNDO

Fedora Argentina Recargada

Con motivos de la unificación de actividades en Latinoamérica, el proyecto Fedora lanzó su nuevo sitio web y lista de correo. Fedora Argentina es una organización no formal que difunde la plataforma Linux a través de la distribución Fedora. Realiza charlas técnicas en universidades, colegios secundarios y colabora en implementaciones en organizaciones sin fines de lucro. http://www.proyectofedora.org/argentina/

IBM OFRECERÁ COMPUTADORAS SIN PRODUCTOS MICROSOFT EN EUROPA ORIENTAL

Según anunció en la feria tecnológica de Hanover, CeBIT 2008, IBM comenzará a vender computadoras en Europa del Este con distintas aplicaciones, que tienen en común que ninguna fue creada por el gigante del software. La nueva línea se llamará Open Referent y tendrá un precio de mercado de hasta un 50 por ciento más bajo que los equipos basados en sistema Microsoft. Para lograrlo se unió a la compañía austriaca VDEL, distribuidora del software Red Hat y con la empresa polaca de servicios y distribución LX Polska. Además los equipos contarán con el software IBM Lotus Symphony, un paquete de aplicaciones, basado en el Open Office y que se presenta como una alternativa al Microsoft Office Open XML.

ACTUALIZACIÓN DEL KERNEL 2.4 PARA DEBIAN 3.1

Debian ha publicado una actualización para el kernel de Debian Linux 3.1 que soluciona múltiples problemas de seguridad en la rama 2.4 del kernel. El proyecto ha lanzado una actualización de la distribución Debian GNU/Linux 3.1, llamada Sarge, la cual agrega principalmente actualizaciones de seguridad. Algunas de las correcciones más importantes se refieren a problemas tales como: Múltiples desbordamientos de memoria intermedia en el subsistema. Bluetooth, fuga de memoria a través de Bluetooth podría permitir a atacantes obtener información sensible, denegación local de servicio a través de etiquetas de flujo entre sockets, fuga de memoria a través del subsistema PPPOE podría permitir a un atacante local consumir toda la memoria y provocar una denegación de servicio, denegación de servicio y potencial ejecución de código en el manejo de memoria de zonas mapeadas, denegación de servicio local

MICROSOFT ABRE SU CÓDIGO

Microsoft anunció que liberara parte del código de sus principales productos para facilitar la interoperabilidad con los productos de la competencia y con los clientes. La misma se basa en 4 pilares fundamentales: crear conexiones abiertas a sus principales productos, promover la portabilidad de datos, aumentar el apoyo para los estándares industriales y buscar mejores relaciones con los clientes y con sus competidores en la industria, incluidas las comunidades de código abierto. En cuanto a los protocolos de comunicación, solo se podrán utilizar gratuitamente sin fines comerciales o de lo contrario se deberán

DEL SOFTWARE LIBRE

Linux Professional Institute

Liberado Mozilla Thunderbird 2.0.0.12

Una nueva revisión de seguridad del Mozilla Thunderbird fue liberada. Principalmente lo que se corrigió fue el desbordamiento de búfer en cuerpos externos MIME, la posible revelación de la información en el decodificador BMP, la vulnerabilidad del directorio trasversal vía chrome: URI y cuelgues con evidencia de corrupción de memoria (rv:1.8.1.12).

http://www.mozilla.com/en-US/thunderbird/

GNOME y Mozilla unen fuerzas

Para mejorar el soporte tanto para desarrolladores como para los usuarios de aplicaciones de escritorio bajo GNU/Linux y otos sistemas operativos, la Fundación GNOME y Mozilla anunciaron un incremento de colaboración. Por lo tanto, la Fundación Mozilla se unirá al comité de asesores de la Fundación GNOME; reafirmará su compromiso de integrar la plataforma de desarrollo XUL con la plataforma de GNOME y cederá U$S 10.000 a la Fundación GNOME para mejorar la accesibilidad del escritorio GNOME bajo el programa GNOME

ECH.com.ar

BREVES

10 amenazas en seguridad informática para 2008

De un informe elaborado por el Sans Institute les mostramos cuáles son las amenazas en materia de seguridad previstas para este año.

1. Ataques cada vez más desarrollados a sitios web, explotando las vulnerabilidades de los navegadores.

2. La creciente sofisticación y eficacia en botnets: En 2008 más variantes y creciente sofisticación mantendrán a este gusano y otros aún más desarrollados como una de las más peligrosas amenazas.

3. Cyber espionaje: En 2008 estos ataques entre Estados y agencias estatales aumentarán además en tiempos en que la información significa dinero también aumentara el robo de datos entre empresas.

4. Ataques contra teléfonos móviles, en especial contra el iPhone y celulares basados en la plataforma Android.

5. Los ataques de abuso de información privilegiada: Se trata de ataques que se inician desde adentro de la organización por empleados, consultores o contratistas.

6. Robo de identidad a través de bots: Capaces de permanecer en las máquinas de tres a cinco meses, recolectando contraseñas, información bancaria, direcciones de correo electrónico de uso frecuente y muchas cosas más.

7. Cada vez más programas malware.

8. Ataques a las vulnerabilidades de la Web 2.0.

9. Phishing cada vez más sofisticados.

10. Ataques contra la cadena de suministro infectando Dispositivos de Consumo (USB Thumb Drives, Sistemas GPS, marcos de fotos, etc) que luego son distribuidos por organizaciones de confianza.

Microsoft lanzó el beta de Internet Explorer 8

En una decisión que tomó por sorpresa a muchos, Microsoft decidió adelantar la liberación de la beta del Internet Explorer 8, la cual ya esta disponible en el sitio de la compañía, algo que no se esperaba hasta junio.
Algunas de las novedades del Explorer 8 son mayor interoperabilidad, la integración de los sitios Facebook y eBay en la barra de navegación y nuevas aplicaciones como el servicio LiveMaps. Además la nueva versión permite guardar en una computadora local, aquellos trabajos que se estaban realizando en un sitio de Internet, si es que se cae la conexión.



El Internet Explorer es el navegador más utilizado del mundo, aunque en los últimos tiempos ha perdido una importante cuota de mercado frente al Firefox de Mozilla.

Llega a la Argentina la laptop más liviana del mundo

Toshiba anunció la disponibilidad en América Latina de la Portege R505, una computadora portátil de sólo 799 gramos de peso que cuenta además con una pantalla LED transflectiva y tecnología EasyGuard, que la protege de golpes y caídas.
Además, se trata de una de las más delgadas del mundo pero no la más, ya que ese honor le pertenece a la MacBook Air. La Toshiba Portage tiene un grosor de 19.5 milímetros, mientras que la MacBook Air mide 0,4 centímetros en su parte más fina y 1,9 centímetros en la parte más gruesa. La Portage cuenta con una pantalla de 12 pulgadas Ultra Brillo Transflectiva, una tecnología que elimina el impacto de reflejos en ambientes con mucha luminosidad.
Cuenta con un disco rígido de 160 GB, un procesador Intel Core 2Duo, 2 GB de memoria RAM, una batería que dura 12 horas, unidad de lectura DVD Super-Multi de 7 milímetros y capacidad para soportar el estándar de comunicaciones que sucederá al WiFi, el WiMax.
En materia de seguridad viene con lector de huella dactilar biométrico. El precio recomendado es de $ 9.999.

Humor *por Severi*




Microsoft
Tu potencial. Nuestra pasión.
1 2 3
4 5 6
7 8 9
0
ENTER